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

# Identity Management (IDM)

# User Guide

**Version 1.13**
**09/04/2024**

**Document Number**: IDM User Guide Version 1.13
**Contract Number**: 47QTCA19D00FF:75FCMC22F0004
**Last Reviewed:** 09/04/2024

# 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 50 states' 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.

## 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 that 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.

## 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 vary depending on their role and includes, but is not limited to:

- Creating an account
- Signing into the IDM system
- Requesting a role
- Identity proofing
- Managing role requests
- Performing account management functions
- Generating reports

## Where to Get Help

Users can quickly find answers to common questions in the Help Center using the **Need Help?** menu and the **Need Help?** link. The **Need Help?** menu is located at the top right corner of the IDM Sign In page and the **Need Help?** link is located at the bottom center of the IDM Sign In page.


**Figure 1: Location of the Help Center Menu and Link**

The Help Center provides answers to the following questions:

- How do I find my Application Help Desk contact information?
- How do I sign in?
- How do I unlock my account?
- How do I change my password?
- How do I add Multi-Factor Authentication (MFA)?
- How do I use the IDM system?
- How to perform Annual Role Certification?

Users that require support beyond what is offered in the Help Center will be referred to the corresponding topic within this user guide.

Application (Tier 1) Help Desk contact information can also be obtained from the CMS Tier 1 Help Desk Support website.

# 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.

## Verify the Web Browser is Supported

The IDM User Interface (UI) is tested for compatibility with current versions of the following modern web browsers:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Safari

## 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.

## Review Account Creation Instructions

All users should receive account creation instructions from their organization or their CMS contact. It is important for the user to review these instructions before starting the account creation process.

# 3. Overview of the IDM System

The following terms are introduced in this section:

- **Role** - A name given to a set of permissions in an application, e.g., Representative, Submitter, or Authorizer. 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, User ID and password creation, and multi-factor authentication (MFA) device setup. It also enables users to manage roles within CMS applications. IDM supports the following types of users along with their most common functions:

**Application End Users:**

Application End Users can:

- Create an account
- Sign into IDM
- Request a role
- Modify, or remove a role
- Perform identity proofing
- Sign into an application
- Manage their profile
- Perform self-service functions, such as:
    - Recover a forgotten User ID
    - Reset a forgotten password
    - Reset an expired password
    - 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
- 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,
- 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 with 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 page.


1) Use the following procedure to begin ***New User Registration***, by navigating to https://home.idm.cms.gov/. The Sign In page appears.

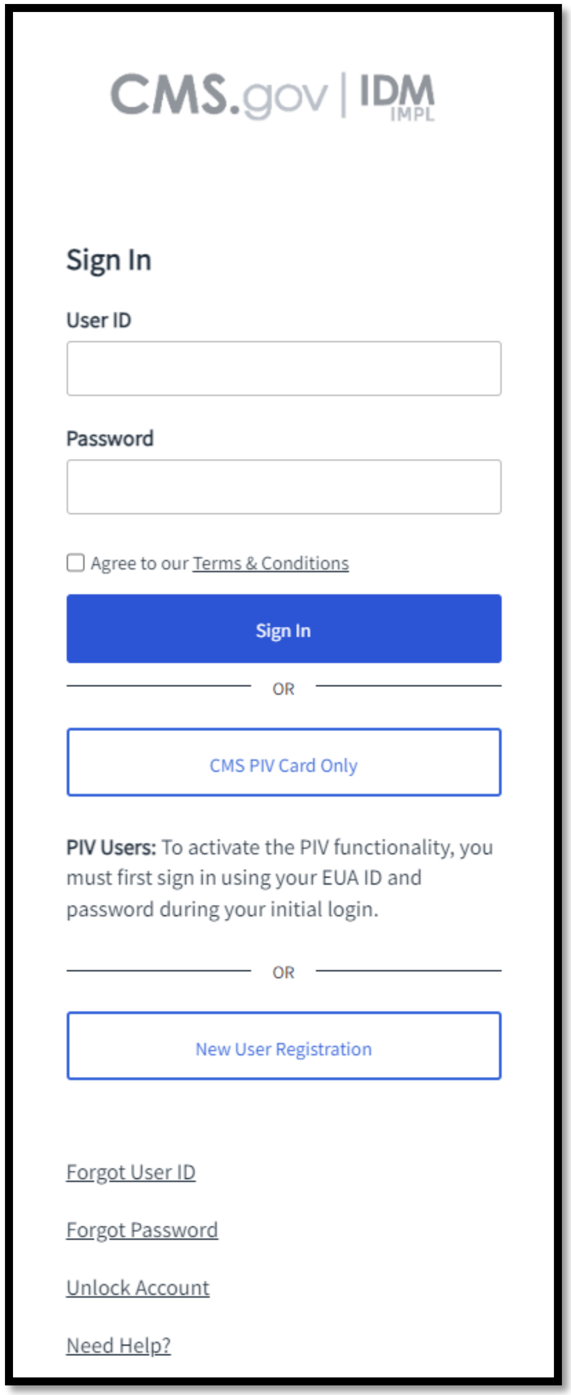



**Figure 2: IDM System Sign In Page**

2) Select 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) Select the ***View Terms & Conditions*** button. Read the IDM System terms and conditions then select the ***Close Terms & Conditions*** button.
7) Select the checkbox to acknowledge agreement with the terms and conditions, then then 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) Select 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. [1]
12) Select a **Security Question** from the list.
13) Type the security question answer into the ***Answer*** dialog box.
14) Select the ***Submit*** button to submit the account registration request. The system will display a message that indicates the account was successfully created.
15) Select 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 during this stage of account creation, it could 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.

[1] 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. Most roles in IDM require MFA. See **Section 11 How to Manage MFA and Recovery Devices** for more information about MFA.

**Note:** Users are encouraged to add multiple MFA devices to their IDM account. If multiple MFA devices are not added during the first sign-in, users can add additional MFA devices using the procedures described in **Section 11 How to Manage MFA and Recovery Devices**.

## How to Sign In (First Time Sign in - All Users)

**Note:** All users who sign in for the first time after creating an account will automatically be prompted to confirm their email as their default MFA device. Users will be prompted to authenticate with an MFA device that is registered to their account each time they sign into the IDM System.

Use the following procedure to sign in.

1) Navigate to https://home.idm.cms.gov, the Sign In window appears as illustrated by **Figure 2: IDM System Sign In** .
2) Enter the User ID and Password.
3) Read the Terms & Conditions, select the checkbox to acknowledge agreement, and then select the ***Sign In*** button. The ***Verify with your Email*** window appears.

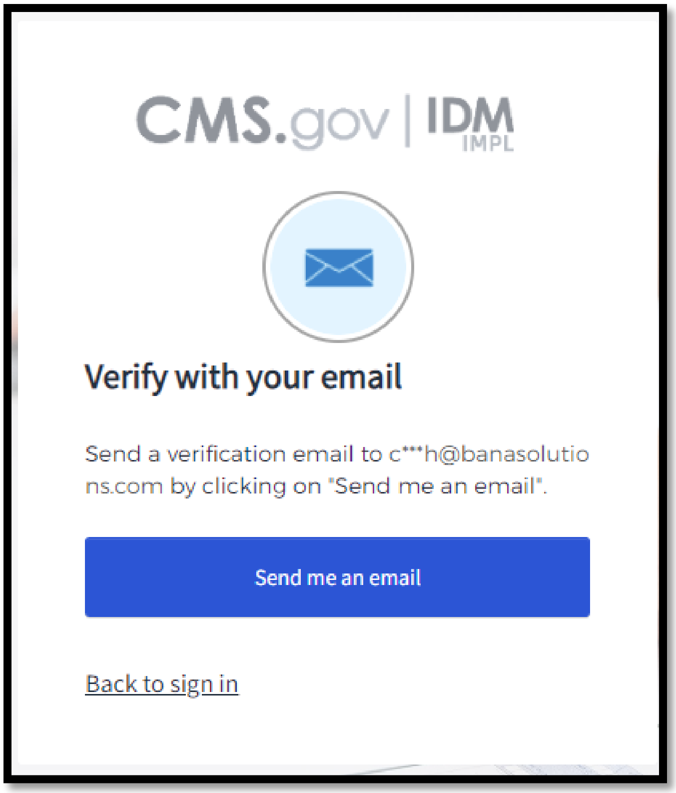


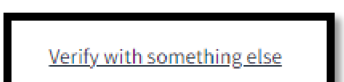

**Figure 3: MFA Setup**

4) Select the ***Send me an email*** button to verify email.
5) Enter the code sent to the email

## 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 2: IDM System Sign In** .
2) Enter the User ID and Password.
3) Read the Terms & Conditions, select the checkbox to acknowledge agreement, and then select the ***Sign In*** button.
4) By default, the user may be prompted to use the last MFA method they used to sign in. In this case, users who have multiple MFA devices registered to their profile can select "**Verify with something else**" and choose a different MFA method they would like to use.




5) Follow the directions for the chosen MFA device to sign in.

## 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.

**Note:** 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 0 How to Sign In (First Time** Sign in - All Users). Thereafter, EUA users who sign in with their EUA ID from a CMS networked computer can sign into IDM using the procedure in this section.

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:

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


2) Select the ***CMS PIV Card Only*** button.

3) Follow the prompts. The IDM Self-Service Dashboard appears after the user is authenticated.

## 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.

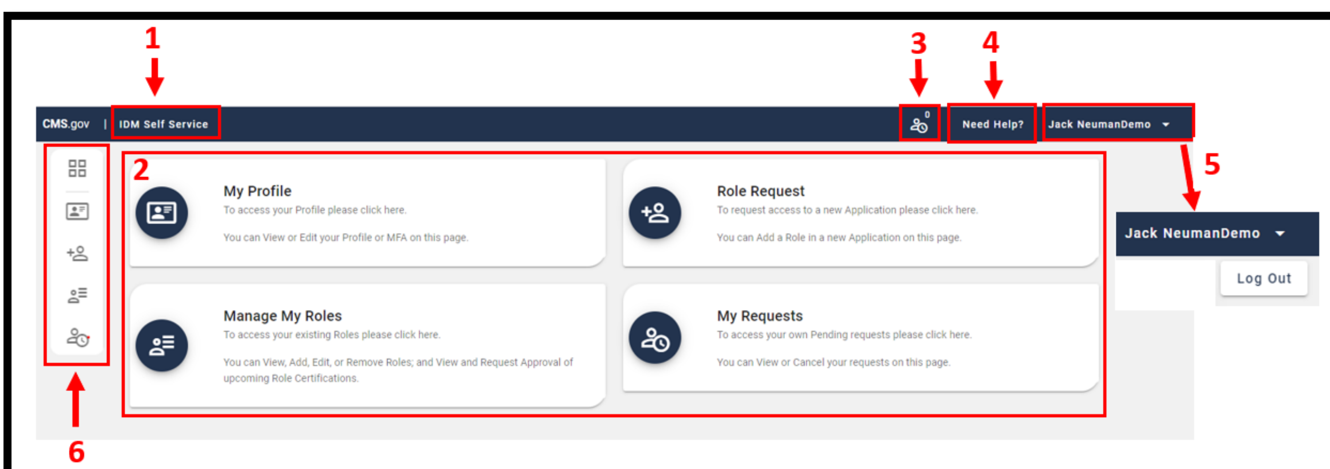



**Figure 4: Self-Service Dashboard Layout**

**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 | Need Help? Button | This button displays the IDM Help Center in a new web browser window. For a description of the Help Center see **Section 0 Where to Get Help**. |
| 5 | Dropdown Menu | This menu displays user's identity and provides access to the Log Out function when selected. |
| 6 | 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. |

## Session Expiration

The **Session Expiring** window appears if a user is signed into IDM but has been inactive for 28 minutes.

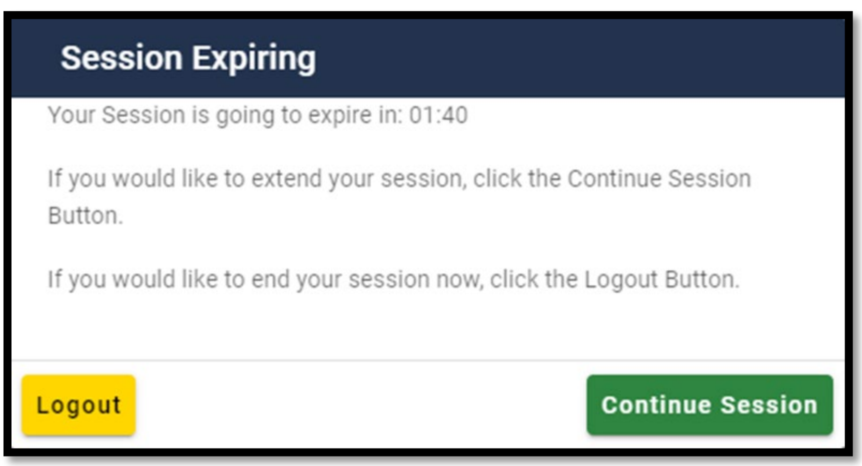



**Figure 5: Session Expiring Window**

If the user selects the ***Continue Session*** button, their session will be extended for another 30 minutes.

If the selects 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.

# 6. How to Request a Role

The following terms are introduced in this section:

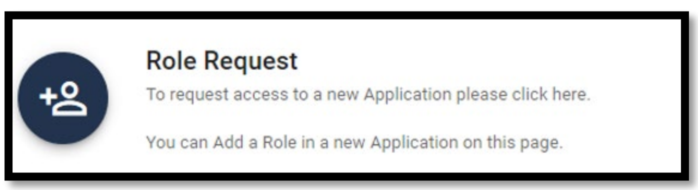
- **Remote Identity Proofing (RIDP)** - Describes the process that is used to confirm a person's identity. Most users will be required to complete RIDP as part of the process of being approved for a role. RIDP is also called Identity Verification. Users may have three opportunities to verify their identity. 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 or phone identity proofing.

## 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.




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

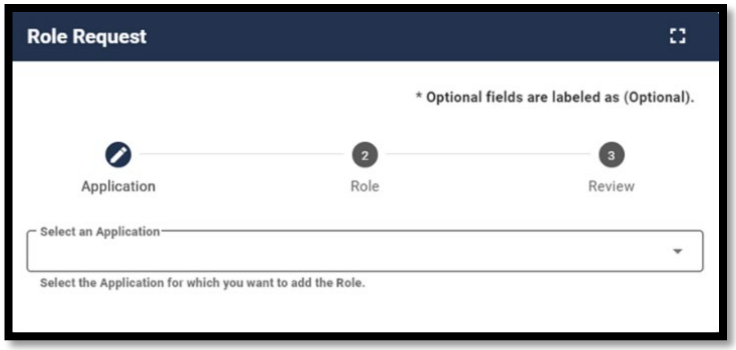



**Figure 6: Role Request Window**

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

3) Select a role. The RIDP window appears after a role is selected.

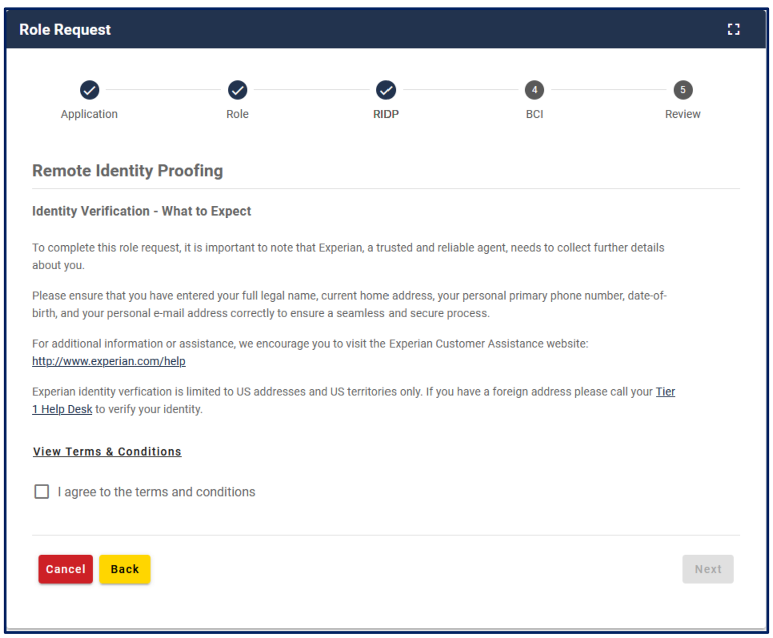



**Figure 7: Role Request - RIDP Terms and Conditions**

4) Review the RIDP terms and conditions, Select the "*I agree to the terms and conditions*" selection box, then select the ***Next*** button. The Identity Verification form appears. Inside the form, fill out all required fields. If "Commonwealth of Puerto Rico" is selected as the state, a pop up will appear offering additional guidance on address formatting.

---

[2] 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) After completing the Identity Verification form, select the ***Submit*** button. The Attribute menu appears.[3]

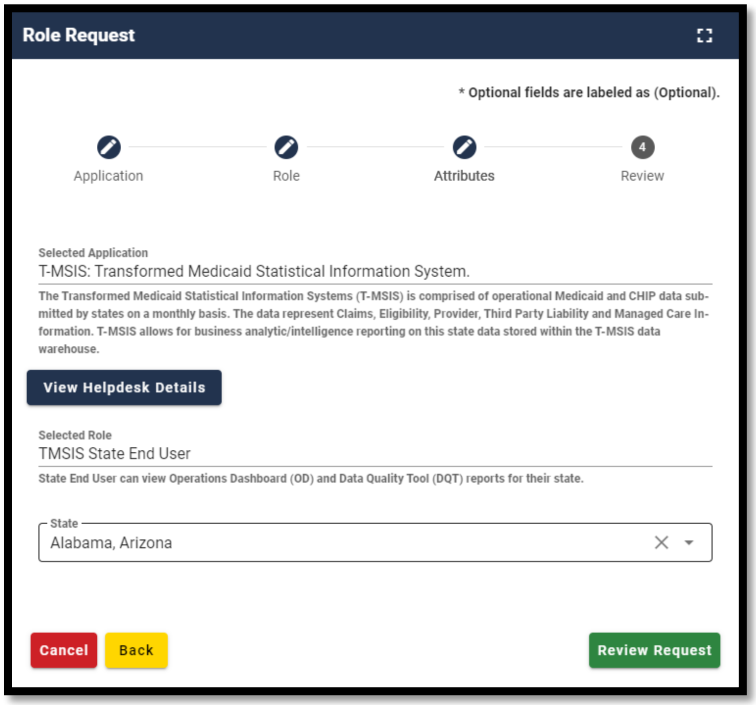



**Figure 8: Role Request - Attribute Selection**

6) Select the required attributes.
7) Review the role request information and select the ***Review Request*** button. The Reason for Request dialog box appears.
8) Enter a justification and select 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.[4]
9) The ***My Requests*** indicator 

on the Self-Service Dashboard increments to display the user's current number of pending requests.
10) Select the ***Back to Home*** button. The user returns to the Self-Service Dashboard.

---

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

[4] 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 9: RIDP Online Proofing Error Message.**

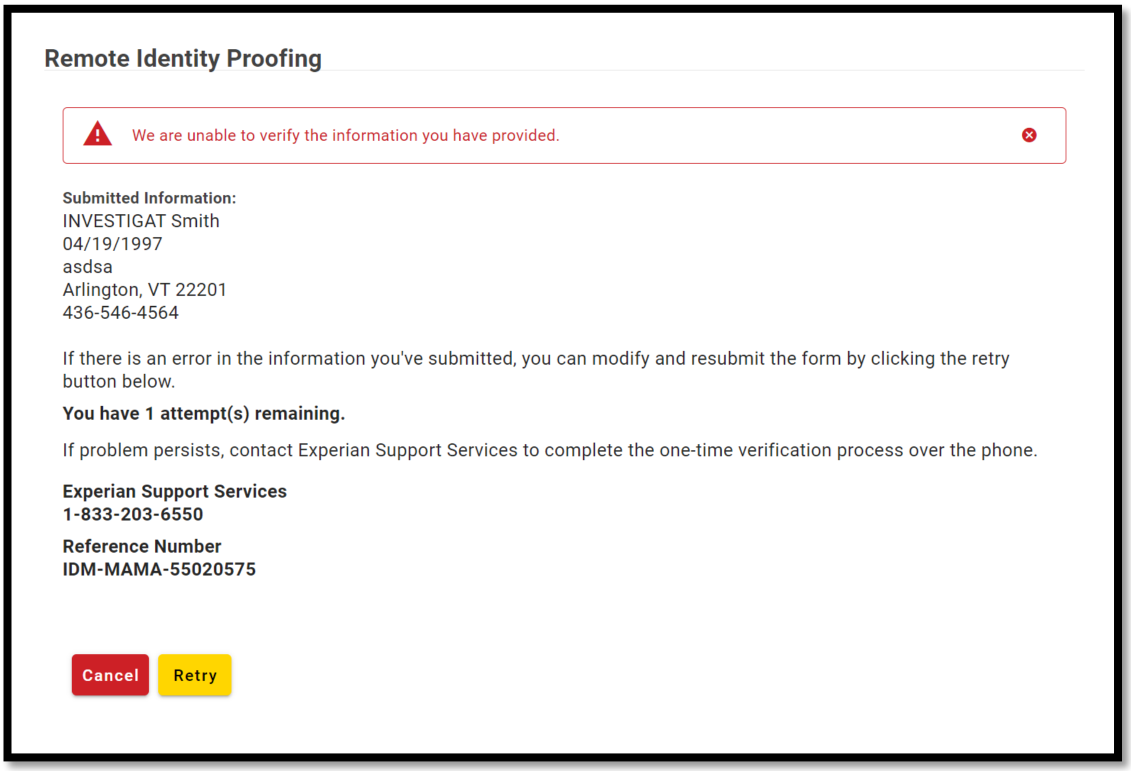



**Figure 9: RIDP Online Proofing Error Message**

1) Write down the Experian support contact information and the Review Reference Number. This information will also be emailed to the user.
2) If there was a mistake in the submitted personal information, select the ***Retry*** button. Proceed from Section 6.1 Step 5.
3) If the info seems correct or need more help is needed, select the ***Cancel*** button. The Confirm Close window appears.
4) Select the ***Confirm Close*** button.
5) Contact Experian using the contact information provided in the error message and perform Phone Proofing.
6) If Phone Proofing was successful, sign into the IDM System and initiate the role request procedure again. When the user reselects the desired role, the Role Request window will display a message which asks if Experian has been contacted.

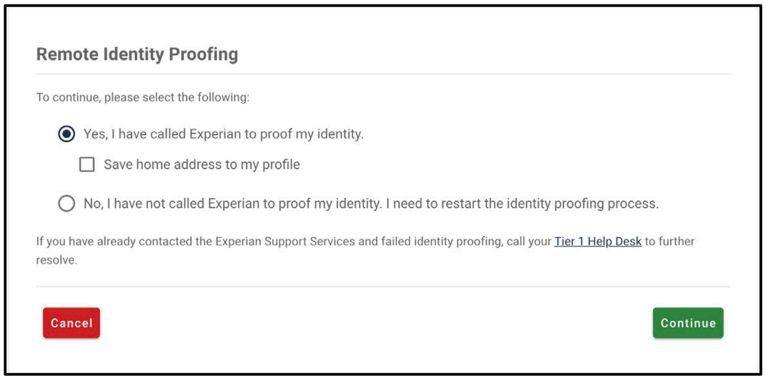



**Figure 10: Experian Phone Verification Confirmation**

7) Select the "*Yes, I have called Experian to proof my identity*" radio button if Experian has been contacted.
    a. Certain personal information provided to Experian will always be saved in the user's profile. This includes name, date of birth, and the last four digits of the user's social security number. If the user wants to save the address provided to Experian to their profile as well, select the "*Save home address to my profile*" checkbox.
8) Select the ***Continue*** button, then select 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 11: Phone Proofing RIDP Error Message**.

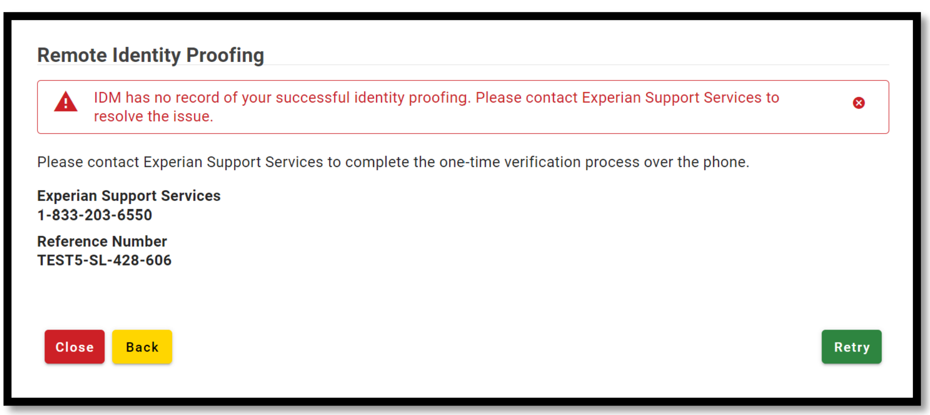



**Figure 11: Phone Proofing RIDP Error Message**

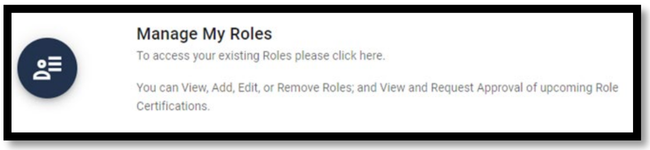
1) Ensure the user has contacted Experian using the contact information provided in the error message and perform Phone Proofing.

2) If Phone Proofing was successful, select ***Back***. Select the "*Yes, I have called Experian to proof my identity*" radio button. Select ***Continue***.
3) If the error persists, 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.

## 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.

1) Select the ***Manage My Roles*** button.




2) The Manage My Roles window appears and displays the user's existing roles.

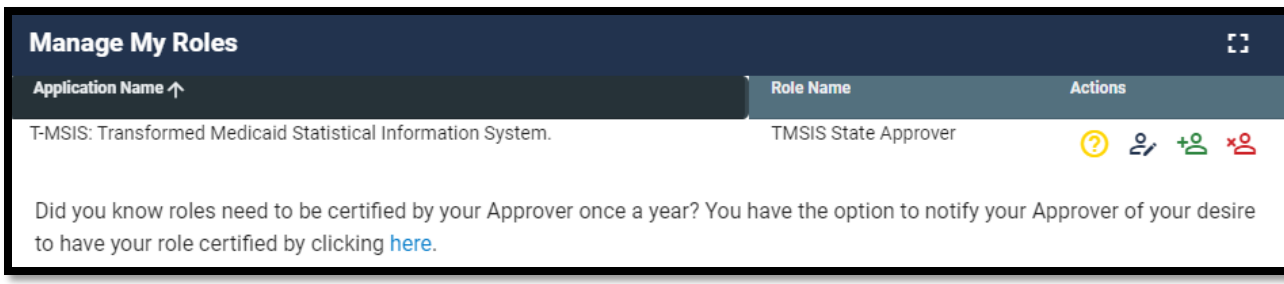



**Figure 12: Manage My Roles Window - User's Existing Roles**

3) Select 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. [5]

[5] 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.

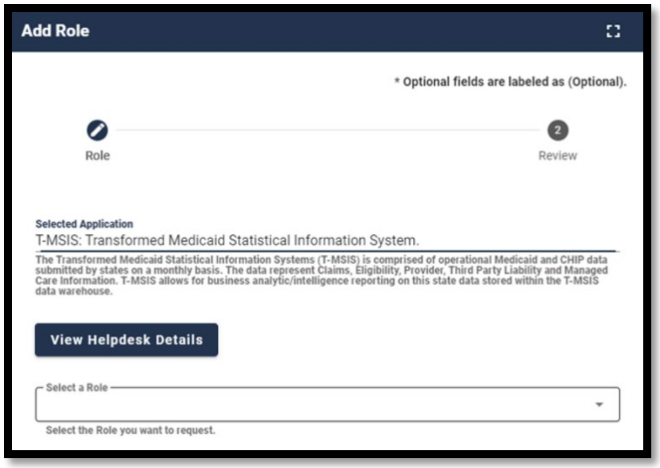



**Figure 13: Add Role Window**

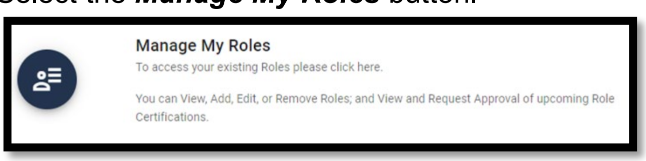
4) Select a Role. The Attribute menu appears.
5) Select the required attributes.
6) Review the role request information and select the ***Review Request*** button. The Reason for Request dialog box appears.
7) Enter a justification and select the ***Submit Role Request*** button. The Role Request window displays the Request ID information and a message that states the request was successfully submitted to an approver for action. [6]
8) The ***My Requests*** indicator 

on the Self-Service Dashboard increments to display the user's current number of pending requests.

## How to Add Attributes to an Existing Role

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

1) Select the ***Manage My Roles*** button.




[6] 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.

2) The Manage My Roles window appears and displays the user's existing roles as illustrated by **Figure 12: Manage My Roles Window - User's Existing Roles.**

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

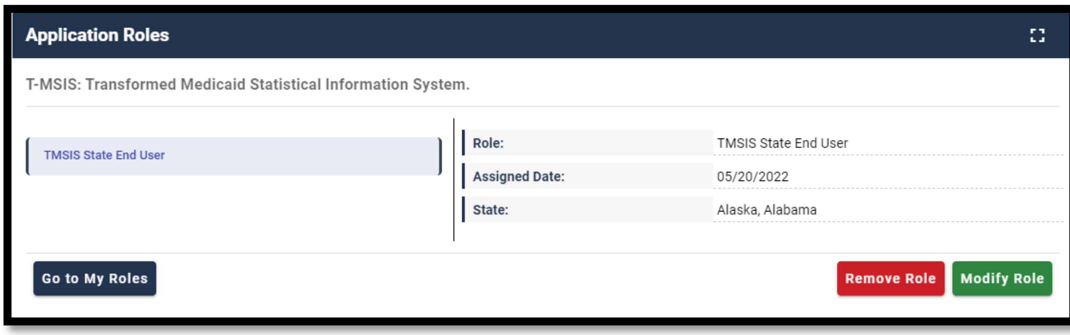



**Figure 14: Application Roles Window - Role Details View**

4) Select 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.
5) Add one or more role attributes.
6) Enter a justification statement and select the ***Submit*** button. The Edit Role Details window displays the Request ID information and a message that informs the user that the request was successfully submitted. [7]
7) Select 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.



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

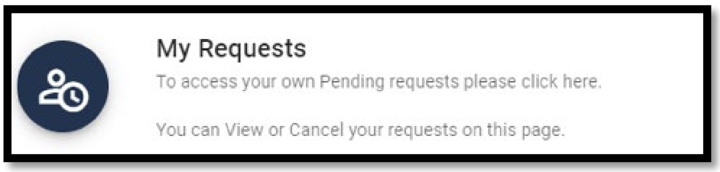
# 7. How to View and Cancel Role Requests

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 selecting 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.

## How to View Role Requests

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




The My Requests window appears and displays the user's pending role requests.[8] [9]

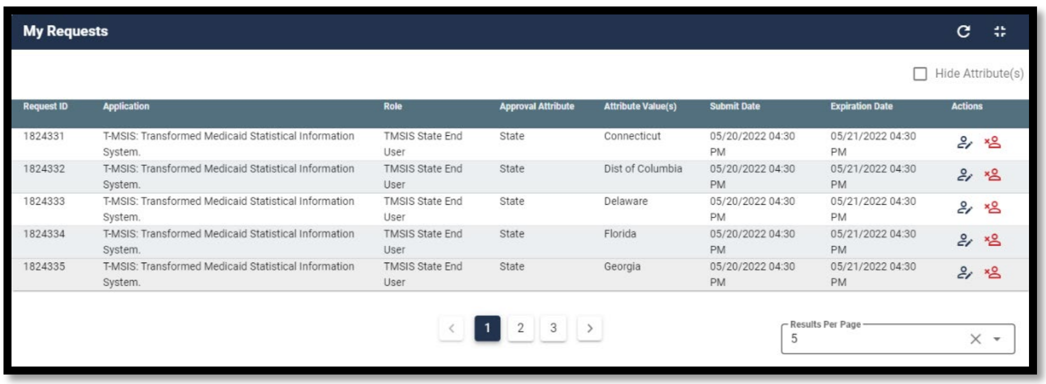



**Figure 15: My Requests - Role Requests Pending Approval**

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

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

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

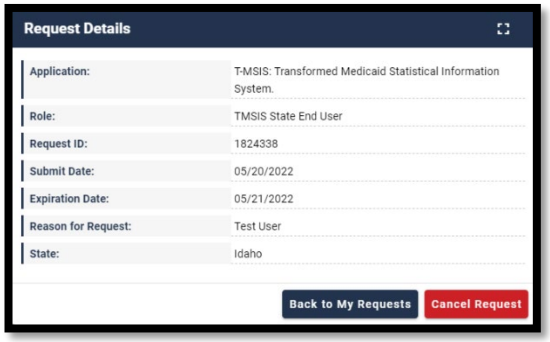
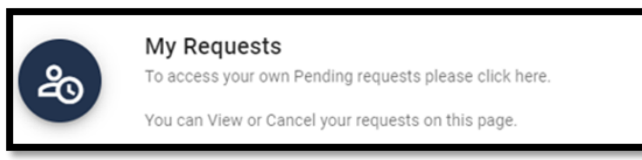



**Figure 16: Request Details Window**

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

## How to Cancel a Role Request




1) Select 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 15: My Requests - Role Requests Pending Approval**.

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

3) Select 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. [10]

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

[10] 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

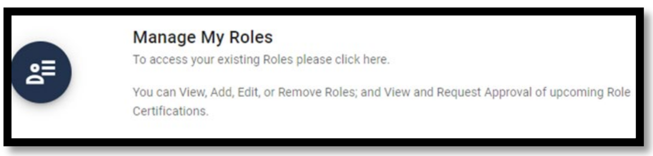
Users remove roles and role attributes using the ***Manage My Roles*** button located on the Self-Service Dashboard.

**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 will remove 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.

## How to Remove a Role

1) Select the ***Manage My Roles*** button.




The Manage My Roles window appears and displays the user’s existing roles.

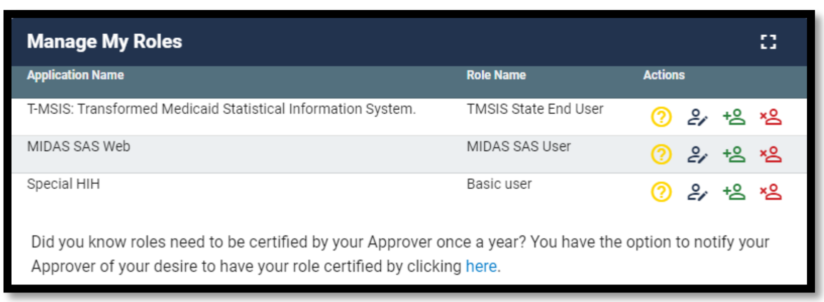


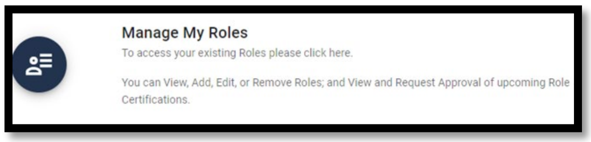

**Figure 17: Manage My Roles Window**

2) Select the **Remove Role** button.  The Remove Role decision window appears.

3) Select 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. [11]
4) Select the ***Go to My Roles*** button. The Manage My Roles window appears and displays the user's current roles.

## How to Remove Attributes From a Role

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




1) Select the ***Manage My Roles*** button. The Manage My Roles window appears and displays the user's existing roles as illustrated by **Figure 17: Manage My Roles Window.**
2) Select the ***View Details*** button.  The Application Roles window appears and displays the role details for the selected role.
3) Select the ***Modify Role*** button. The Edit Role Details window appears. [12]

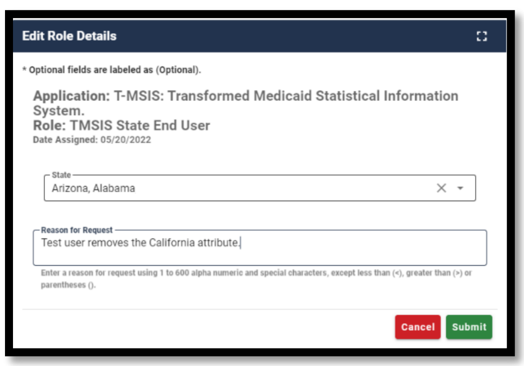



**Figure 18: Edit Role Details Window**

4) Remove the desired role attributes.

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

[12] 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.

5) Enter a justification statement and select the ***Submit*** button. The Edit Role Details window displays Request ID information and a message that informs the user that the request was successfully submitted. [13]
6) Select the ***Go to My Roles*** button. The Manage My Roles window appears and displays the user's current roles.

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

# 9. How to Initiate a Role Certification Request

IMPORTANT: The role certification request procedure is completely OPTIONAL for all users. Approvers are responsible for reviewing and recertifying a user's role(s) even if the user does not request it using the procedure described in this section.

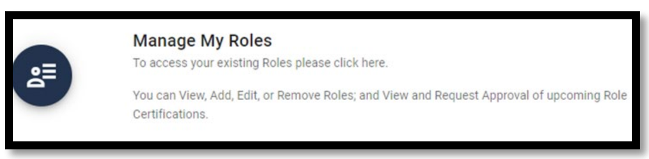
The following terms are introduced in this section:

- **Annual Role Certification** - The process by which a user is granted continued use of a role for another 365 days. Annual Role Certification is required every year by CMS' security policy and is counted from the original role approval date or the previous year's certification date.

The IDM System enables users to send an annual role certification request to their approver for roles which they have a continuing need to access.

**Note:** One email is sent for all the roles due on the same day for the same application. For example, if three roles are due on the same day for the same application, the approver will get one email for that day. But if there is one role due in each of three applications on the same day and there is one approver for all three applications, then the approver will get three emails.

Users initiate annual role certification requests using the ***Manage My Roles*** button located on the Self-Service Dashboard within the Manage My Annual Role Certifications function.




1) Select the ***Manage My Roles*** button. The Manage My Roles window appears as shown in **Figure 19: Manage My Roles Window with Manage My Annual Role Certifications Hyperlink** and displays the user's existing roles. It also displays a hyperlink that provides access to the Manage My Annual Role Certifications function.

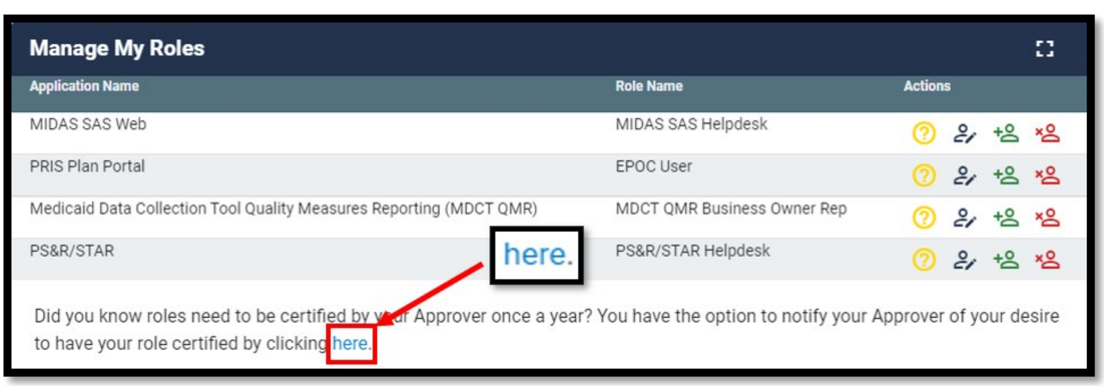



**Figure 19: Manage My Roles Window with Manage My Annual Role Certifications Hyperlink**

2) Select the ***Here*** hyperlink. 

The Manage My Annual Role Certifications window appears and displays a list of the user's roles.

**Note:** Some roles will not be listed here because not all applications use IDM for role recertification. Please contact your helpdesk if you need further assistance.

**Note:** Users may only request certification for roles that have a status of "Certification Due", which means the role is within 120 days of the certification due date.

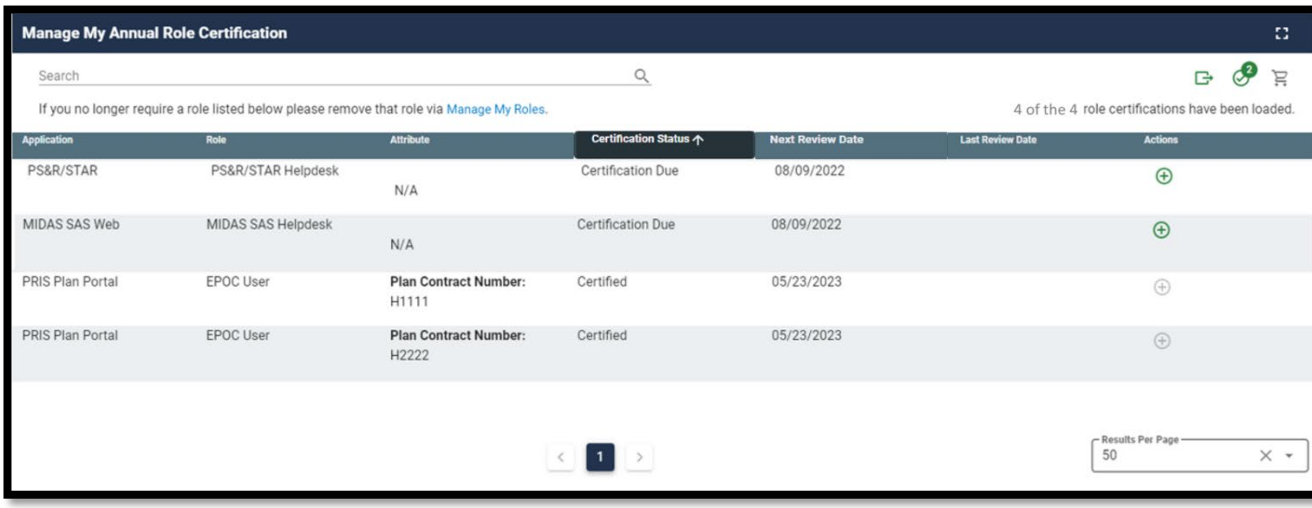



**Figure 20: Manage My Annual Role Certifications Window**

3) Use the ***Search*** Box 

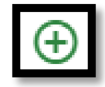
to search for "Certification Due". This filters the list to display only those roles that have a certification status of "Certification Due" (Optional).

4) Select the ***Certification Status*** 

report heading to display all roles with a Certification Status of "Certification Due" at the top of the report (Optional).

5) **Request certification for all roles**: Select the ***Submit All*** button 

to add all roles that are in Certification Due status to the Cart. The Certification(s) to Request window appears. Skip to Step 6 (Optional).

6) **Request certification for individual roles:** Select the ***Add to Cart*** button  to add individual roles that are in Certification Due status to the Cart.

7) Select the ***View Cart*** button.  The Certification(s) to Request window appears.



8) Select the ***Remove from Cart*** button.  to remove the role from the certifications to request list (Optional).

9) ) Provide a Justification of why the role is needed for another year within the Justification field on the Certification(s) to Request window (Optional.

10) Select the ***Submit*** button. The Manage My Annual Role Certification window displays a message that informs the user that the request was successfully submitted.

# 10. 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 following Self-Service features are available as links at the bottom of the IDM Sign In window:

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

Additionally, IDM automatically guides the user through the password update process when their password expires.

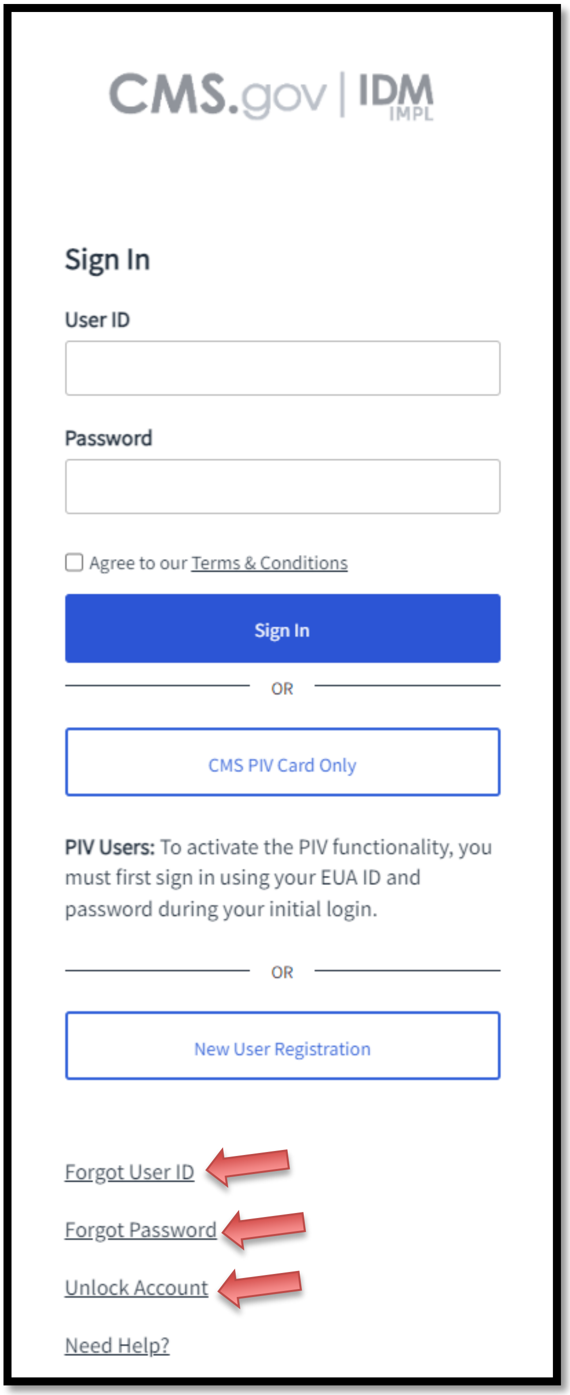



**Figure 21: IDM Sign In Window with Self-Service Links**

**Note:** Users are required to set up MFA factor upon first sign in as described in **Section 11 How to Sign In.**

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.

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.

## 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 22: 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 into the IDM System.

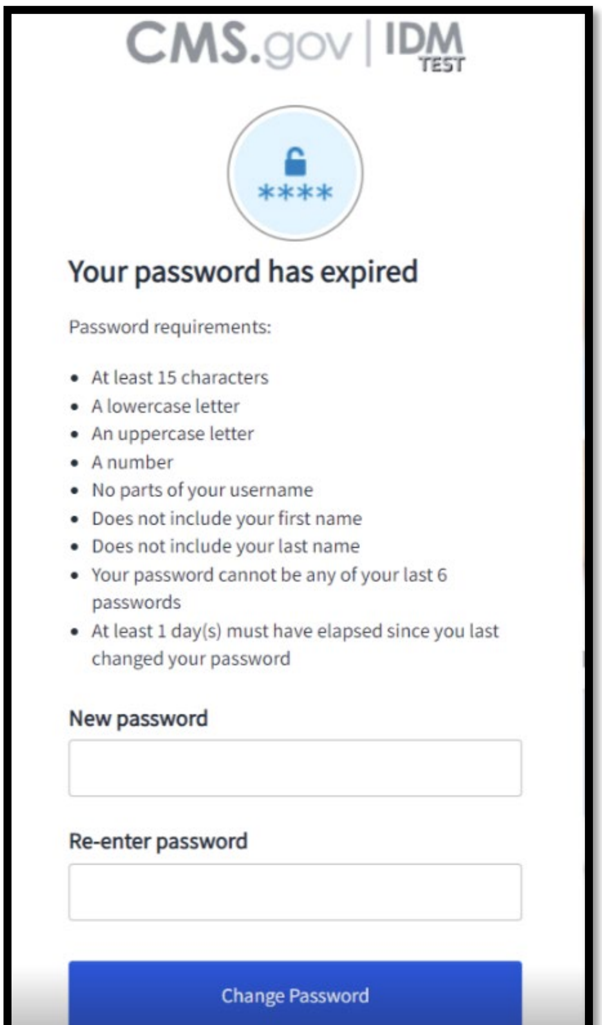



**Figure 22: IDM Self-Service Change Expired Password Window**

1) Enter the New Password and the Repeat Password.
2) Select the ***Change Password*** button.[14]

The User can now sign in using the new password.

## 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 21: IDM Sign In Window with Self-Service Links**.

1) Select the ***Forgot password*** link. The Reset Password window appears.

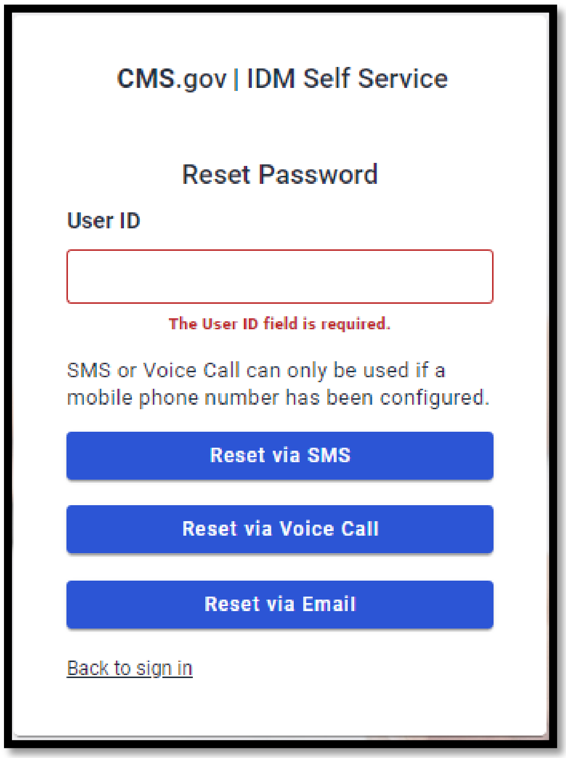



**Figure 23: IDM Self-Service Reset Password Request**

2) Enter the User ID.
3) Select 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.

[14] 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.

4) Select 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. [15]
5) Select 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 select the ***Reset Password*** button. The screen refreshes and the user is prompted to enter a new password.

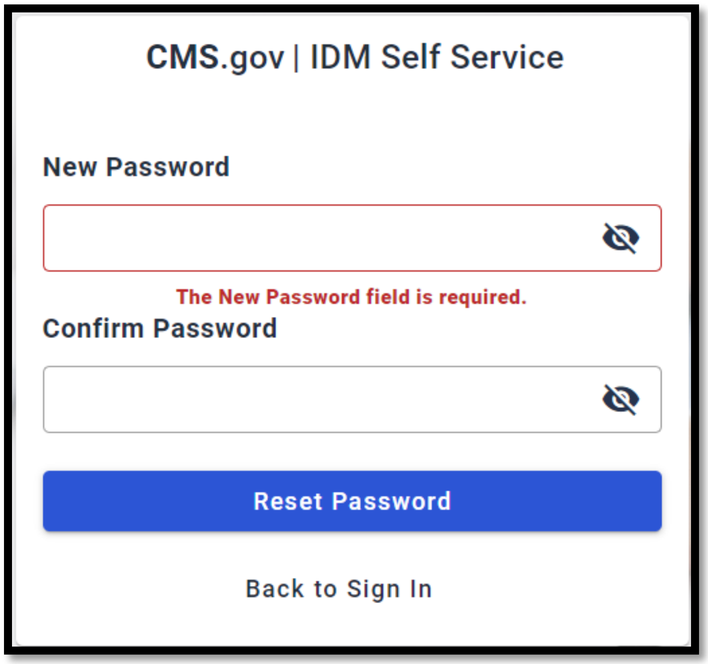



**Figure 24: IDM Self-Service Reset Password Set New Password**

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

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

## Recover a forgotten User ID

Users who forget their User ID can recover it using the ***User ID*** link located at the bottom of the IDM Sign In window as illustrated in **Figure 21: IDM Sign In Window with Self-Service Links**.

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

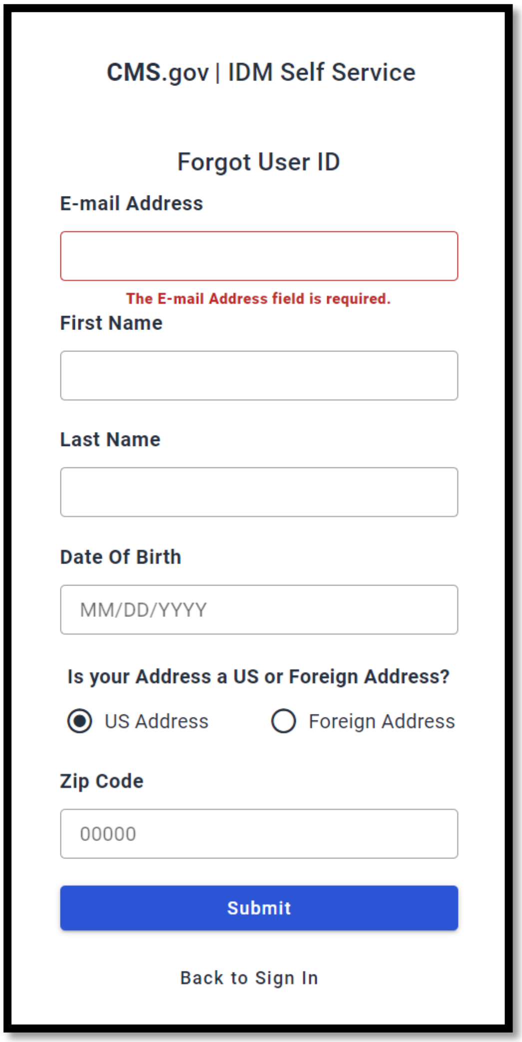



**Figure 25: IDM Self-Service Forgot User ID Window**

2) Enter the E-mail Address, First Name, Last Name, and Date of Birth.
3) Keep the default "***US Address***" setting if the address is a US address. If the address is foreign, select the "***Foreign Address***" radio button control.

4) Enter the Zip Code and select 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. [16]
5) The IDM System sends an email to the email address listed in the user's profile. This email contains the user's User ID.
6) Select the ***Back to Sign In*** button. The user returns to the IDM Sign In window.

## 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 26: 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 21: IDM Sign In Window with Self-Service Links**.

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. If the user takes no action, their account will automatically unlock after one hour.

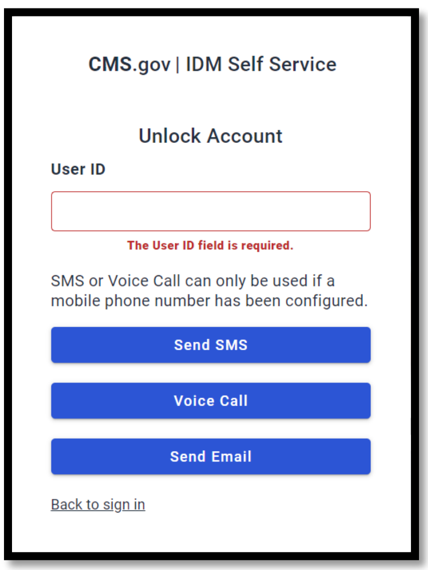



**Figure 26: IDM Self-Service Unlock Account Window**

1) Enter the User ID.
2) Select the ***Send Email*** button. The Unlock Request Sent window appears.
3) Select the ***Back to Sign In*** button.

---

[16] 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.

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.
5) Select 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 select the ***Unlock Account*** button. The screen refreshes and displays a message which states that the account was successfully unlocked.
7) Select the ***Back to Sign In*** button. The IDM System Sign In window appears and the user's account is now unlocked.

# 11. 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** - Recovery Device – An MFA device that is used to authenticate a user during the recovery process. These MFA devices serve as recovery devices: Email, Short Message Service (SMS), and Interactive Voice Response (IVR).

Users are strongly encouraged to register more than one MFA device so that they have alternatives in the event one device is unavailable or does not respond in a timely fashion. For example, when the user does not have possession of their phone, they can still use email. Conversely, if the user's email is not responding, they can use SMS to their phone.

**Note:** When a user uses one phone number for both SMS and IVR, if they remove one of those, then the system removes them both. To avoid this, a user can use two different phone numbers for IVR and SMS.

Changes to MFA/Recovery devices are accompanied by an email notification to the user's email address on record.

**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.

Error! Not a valid bookmark self-reference. lists the MFA and Recovery devices that are supported by the IDM System. [17]

**Table 2: MFA and Recovery Device Summary**

| MFA Device | Device Type | Actions | Modifiable Setting | Edit Settings |
|---|---|---|---|---|
| Email | MFA & Recovery | Add or Remove. | N/A | Edit is not applicable. |
| Text Message (SMS) | MFA & Recovery | Add, Activate, or Remove. | Mobile Phone Number | User can activate a device that is in pending status. |

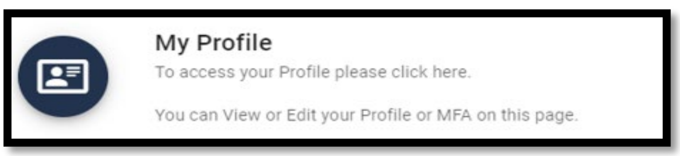
[17] Email, Text, and IVR MFA devices also function as Recovery devices that can be used to recover a forgotten password or unlock an account if the user has registered those devices to their account.

| MFA Device | Device Type | Actions | Modifiable Setting | Edit Settings |
|---|---|---|---|---|
| Interactive Voice Response (IVR) | MFA & Recovery | Add, Activate, or Remove. | Phone Number | User can activate a device that is in pending status. |
| 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.

### How to View MFA and Recovery Devices

1) Select the ***My Profile*** button.




2) The My Profile window appears.
3) Select 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.[18]

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

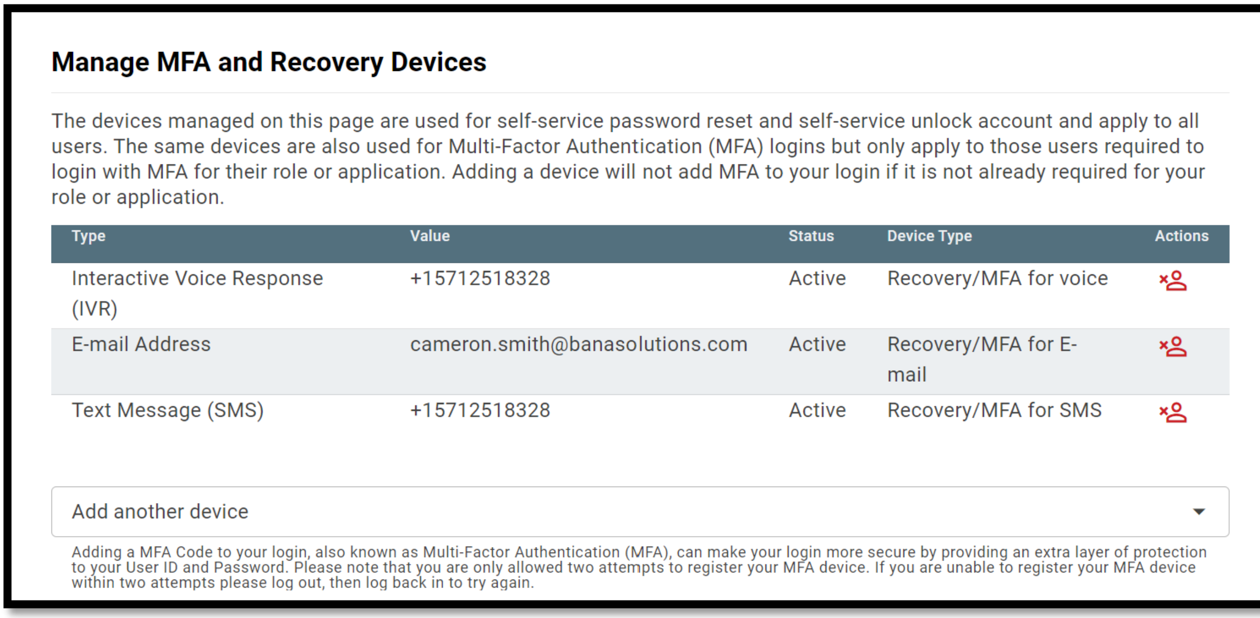



**Figure 27: Manage MFA and Recovery Devices Window**

## How to Add an IVR or SMS MFA/Recovery Device

Users add an 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 0**

2) **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.

3) How to View MFA and Recovery Devices. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 27: Manage MFA and Recovery Devices Window**.

4) Use the ***Add another device*** menu to select the Interactive Voice Response (IVR) option or Text Message (SMS) option. The device configuration window appears.

5) Enter the phone number, (plus extension if applicable) for an IVR or SMS MFA/Recovery device.

6) Select the ***Verify MFA*** button. The MFA confirmation window appears.

7) The IDM System sends a one-time verification code to the user by voice message or text.

8) Enter the one-time verification code and select the ***Confirm MFA*** button. The system displays a message which states that the MFA device was successfully added.

9) Select the ***OK*** button.

## How to Activate a Pending IVR or SMS MFA/Recovery Device

An 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 0**

2) **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.

3) How to View MFA and Recovery Devices. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 27: Manage MFA and Recovery Devices Window**.

4) Select the ***Activate Factor*** button.  The Activate Factor window appears and displays a message which indicates that an MFA code has been sent.

5) The IDM System sends a one-time verification code to the MFA device that is being activated.

6) Enter the one-time verification code and select the ***Confirm MFA*** button. The system displays a message which states that the MFA device was successfully added.

7) Select the ***OK*** button.

## 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.

**1)** Access the Manage MFA and Recovery Devices window using the procedure in **Section 0**

2) **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.

3) How to View MFA and Recovery Devices. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 27: Manage MFA and Recovery Devices Window**.

4) Use the ***Add another device*** menu to select the Google Authenticator option. The Google Authenticator registration window opens.

5) Select the ***Next*** button and follow the on-screen prompts for installing a Google Authenticator MFA device.

6) Download and install the Google Authenticator mobile app onto the mobile device. Obtain the app from the appropriate app store. [19]
7) Select the ***Register Device*** button on the IDM Google Authenticator setup window. The window displays a QR code.
8) Start the Google Authenticator app on the mobile device and select the ***Get Started*** button. The Account Setup screen appears.
9) Select 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. [20]
10) Enter the one-time verification code into the IDM Confirm MFA Code dialog box and select the ***Confirm MFA*** button. A message is displayed that indicates the MFA device was successfully added.
11) Select the ***OK*** button.

### 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 0**
2) **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.

3) How to View MFA and Recovery Devices. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 27: Manage MFA and Recovery Devices Window**.
4) Use the ***Add another device*** menu to select the Okta Verify option. The Okta registration window opens.
5) Select the ***Next*** button and follow the on-screen prompts for installing an Okta Verify MFA device.

---

[19] 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.

[20] Users who are unable to scan the QR code may select 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.

6) Download and install the Okta Verify app onto the mobile device. Obtain the app from the appropriate app store. [21]
7) Select the ***Register Device*** button on the IDM Okta Verify setup window. The window displays a QR code.
8) Start the Okta Verify app on the mobile device. The Welcome to Okta Verify screen appears.
9) Select the ***Add Account*** button on the Okta Verify mobile app, then choose the **Organization** account type.
10) Scan the QR Code using the Okta Verify mobile app. [22]
11) A message is displayed which indicates the MFA device was successfully added. Select the ***OK*** button.

[21] 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.

[22] Users who are unable to scan the QR code may select 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.

## 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 0**
2) **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.
3) How to View MFA and Recovery Devices. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 27: Manage MFA and Recovery Devices Window**.
4) Use the ***Add another device*** menu to select the YubiKey option. The YubiKey registration window opens.
5) Select the ***YubiKey Passcode*** field.
6) 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.
7) Select the ***Confirm YubiKey*** button. A message is displayed which indicates the MFA device was successfully added. Select the ***OK*** button.

## 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) Select the ***My Profile*** button as described in **Section 0 How to Open and Close the My Profile Function.** The My Information window appears**.**


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

3) Select the ***Edit*** button.  The Personal Contact Information becomes modifiable.
4) Enter the new Email Address and select the ***Submit*** 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.

## How to Remove an MFA Device

Users may remove MFA devices using the Manage MFA and Recovery Devices window and the following procedure. [23]

**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 0**
2) **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.

3) How to View MFA and Recovery Devices. The Manage MFA and Recovery Devices window opens as illustrated by Figure 27: Manage MFA and Recovery Devices Window.

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

4) Select the ***Remove Factor*** button  for the MFA device that requires removal. The Remove MFA Device decision window appears.
5) Select the ***Remove MFA Device*** button.

# 12. How Manage User Account Profile Information

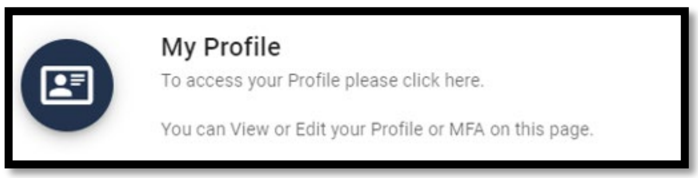
Users view and edit their user account profile information using the IDM Self-Service My Profile Function. This function enables users to view and/or modify various attributes of their user profile to include:

- 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.

## How to Open and Close the My Profile Function

**Open the My Profile Function:**

1) Select 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.
   - Select 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.

## 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) Select the ***My Profile*** button as described in **Section 0 How to Open and Close the My Profile Function.** The My Information window appears.

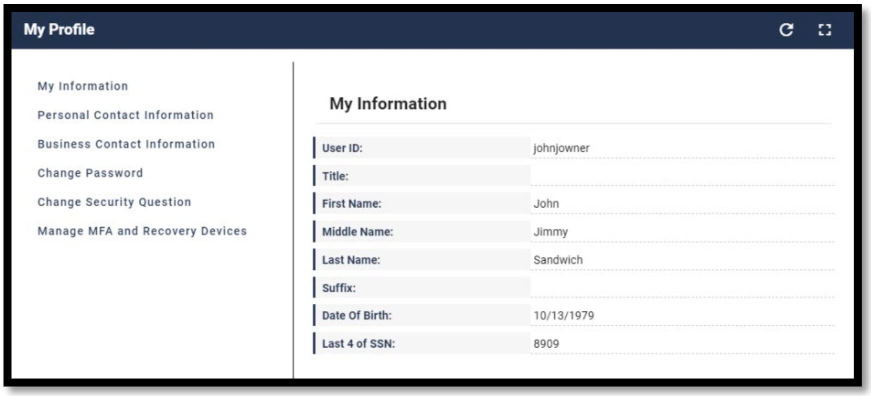



**Figure 28: My Profile - My Information**

# 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) Select the ***My Profile*** button as described in **Section 0 How to Open and Close the My Profile Function.** The My Information window appears**.**


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

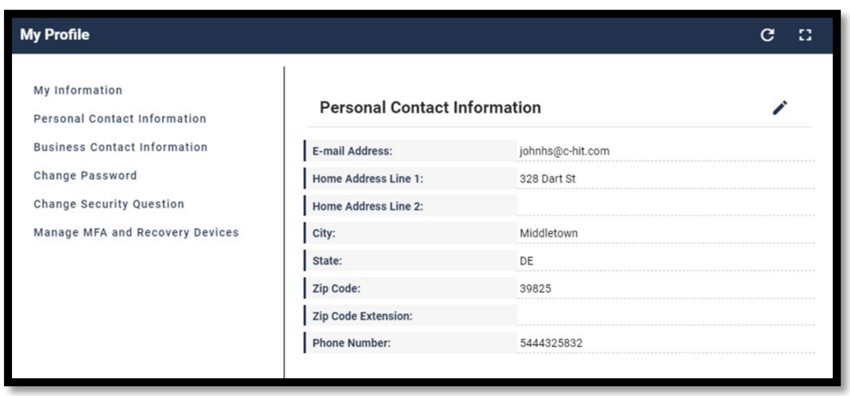



**Figure 29: My Profile - Personal Contact Information**

## Modify Personal Contact Information

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

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

## 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) Select the ***My Profile*** button as described in **Section 0 How to Open and Close the My Profile Function.** The My Information window appears**.**


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

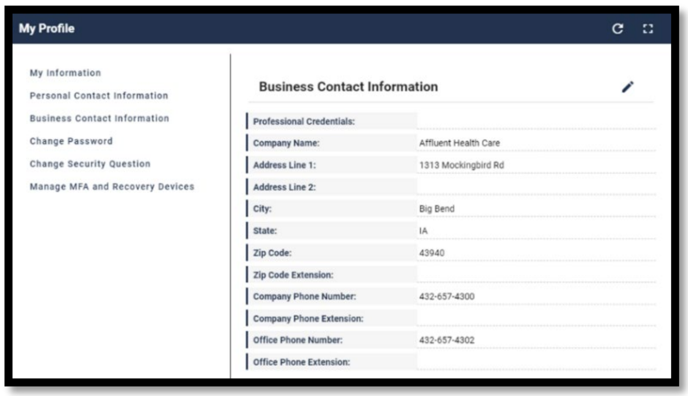
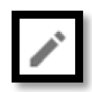



**Figure 30: My Profile - Business Contact Information**

### Edit the User's Business Contact Information

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

## How to Change the User Account Password

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

1) Select the ***My Profile*** button as described in **Section 0 How to Open and Close the My Profile Function.** The My Information window appears**.**
2) Select the Change Password button. 

The Change Password window appears.

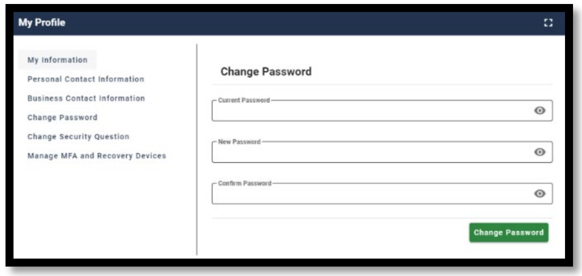



**Figure 31: My Profile - Change Password Form**

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

## 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) Select the ***My Profile*** button as described in **Section 0 How to Open and Close the My Profile Function.** The My Information window appears**.**


2) Select the ***Change Security Question*** button. The Change Security Question window appears.


**Figure 32: My Profile - Change Security Question Form**

3) Select a Security Question from the list.
4) Enter the security question answer into the Answer field. [24]
5) Enter the Current Password.
6) Select the ***Change Security Question*** button.

[24] 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.

# 13. How to Approve Role Requests

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:

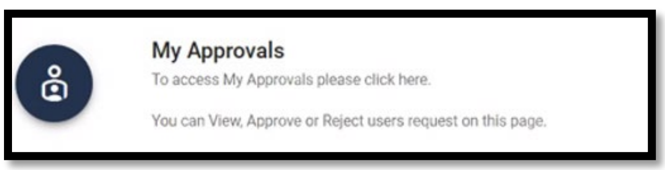
- View a list of all requests pending approval.
- View the details of a specific request pending approval.
- Approve or reject individual requests pending approval.
- Simultaneously approve and/or reject multiple requests pending approval.
- Export a list of requests pending approval.

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

## How to Open and Close the My Approvals Function

### Open the My Approvals Function:

Select the My Approvals button located on the Self-Service Dashboard.




The My Approvals window opens. [25]

[25] The user can also view their pending approvals by selecting the ***My Approvals*** indicator

located at the top right corner of the Self-Service Dashboard.

### Close the My Approvals Function:

1) Choose one of the following actions to close the My Approvals function.
   - Select 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.

## 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) Select the ***My Approvals*** button as described in **Section 0 How to Open and Close the My Approvals Function.** The My Approvals window appears.

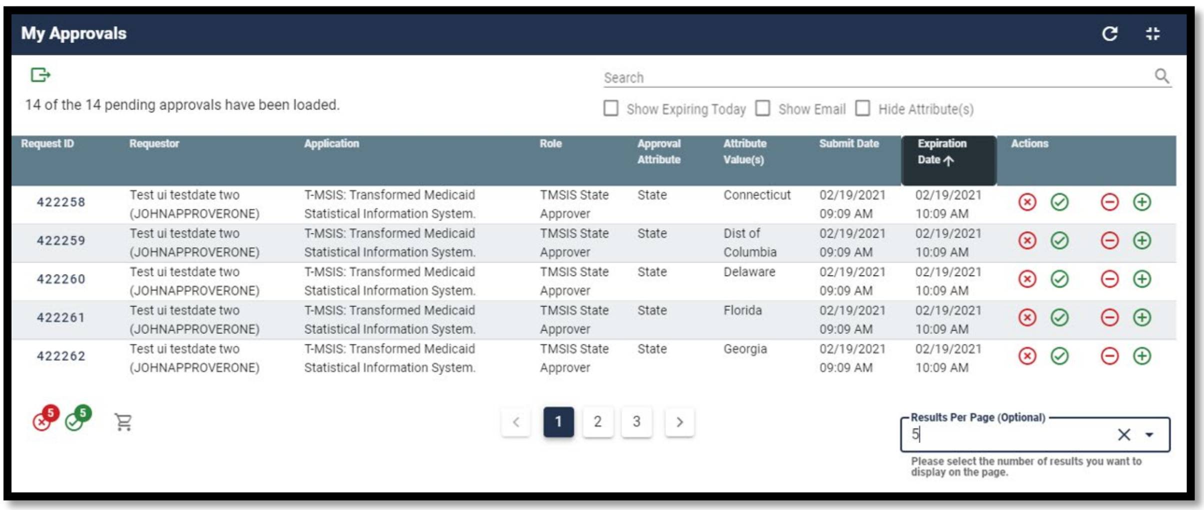



**Figure 33: My Approvals Window**

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. [26]

[26] 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.

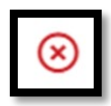
### 13.1.1 How to View Details for a Specific Pending Approval Request

1) While viewing records in the My Approvals window, select the ***Request ID*** 

for the desired record that is displayed in the My Approvals window. The Pending Approval Details window appears.
2) Select the ***Go to My Approvals*** button to close the Pending Approval Details window. The Approver returns to the My Approvals window. [27]

## 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.

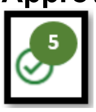
1) Select the ***My Approvals*** button as described in **Section 0 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by Figure 33: My Approvals Window.
2) Select the appropriate button to approve or reject the desired request.
   - **Approve the Request**: Select 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**: Select 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) Select the ***Submit*** button. The IDM System displays a message which indicates the operation completed successfully. The My Approvals indicator decrements by one.
5) Select the ***Go to My Approvals*** button. The Approver returns to the My Approvals window.

[27] The Pending Approval Details window also provides the capability to approve or reject a single request that is pending approval. Refer **Section 13.3 How to Approve/Reject a Single Request.**

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

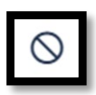
Approvers approve or reject multiple pending requests that are displayed on a single page of requests using the ***Approve All on Current Page Now*** and ***Reject All on Current Page Now*** buttons on the My Approvals window and the following procedure.

1) Select the ***My Approvals*** button as described in **Section 0 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 33: My Approvals Window**.
2) Use the ***Pagination*** control 

to change the number of requests that are displayed on a page in the My Approvals window (Optional).
3) Select the appropriate button to approve or reject all requests on the current page:
   - **Approve the Request**: Select the ***Approve 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 APPROVE.
   - **Reject the Request**: Select 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) Select the ***Request Details*** button 

to view details about a specific request. Select the ***Request Details*** button again to close the details window for that request (Optional).
5) Select the ***Remove Request*** button  to remove a specific request from the Approve or Reject list (Optional).[28]
6) Enter a brief justification. The same justification will be applied to each request.
7) Select the ***Submit*** button. All records that appear on the Pending Approvals to Process list will be processed as Approvals or Rejections.

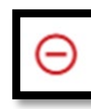
[28] The specific record will be removed from the Pending Approvals to Process list and will remain in pending status. The Approver will receive periodic email reminders about the pending requests until they are acted on, or they expire.

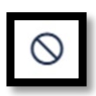
8) The IDM System displays a message that indicates the operation completed successfully and the My Approvals indicator is decremented by the number of requests that were processed.
9) Select the ***Go to My Approvals*** button. The Approver returns to My Approvals window.

## 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) Select the ***My Approvals*** button as described in **Section 0 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 33: My Approvals Window**.
2) Use the ***Pagination*** control 

to change the number of requests that are displayed on each page in the My Approvals window (Optional).
3) Select the appropriate button to approve or reject each individual request that is displayed on the page:
    - **Approve the Request**: Select 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**: Select 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.
4) Select the ***Cart*** button. 

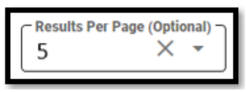
The Pending Approvals to Process window appears.
5) Select the ***Remove Request*** button  to remove a specific request from the bulk Approval/Rejection action (Optional).[29]

[29] 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.

6) 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.
7) Select 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 which indicates the operation completed successfully and the My Approvals indicator is decremented by the number of requests that were processed.
9) Select the ***Go to My Approvals*** button. The Approver returns to the My Approvals window.

## How to Export a List of Pending Approvals to an Excel Spreadsheet

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) Select the ***My Approvals*** button as described in **Section 0 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 33: My Approvals Window**.
2) Use the ***Pagination*** control 

to adjust the number of requests that are displayed on each page (Optional).
3) Use the ***Search*** box 

to perform a search across all columns to obtain a list of records that contain a desired alphanumeric search term (Optional).
4) Select the ***Expiring Today*** filter 

to display only those requests that will expire on the current day (Optional).
5) Select the ***Hide Attributes*** filter 

to hide or view the columns of information that pertain to role attributes (Optional).
6) Select 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 selects (Optional).
7) Select the ***Export*** button and select the output format.  The Save As window opens.
8) Select the ***Save*** button. The list of pending approvals is downloaded to the user's computing device as a Microsoft Excel spreadsheet (.xls) file.

# 14. How to View IDM Reports

## Description of the IDM Reports Function

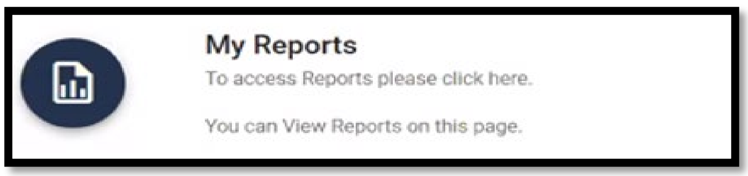
Users who require access to the IDM Reports must submit a role request for the IDM Reports application using the procedure outlined in **Section 0 How to Request a Role for a New Application**.

**Note:** Users will receive access to a predetermined number of reports based on the specific role that they request. **Appendix B: Summary of IDM** Reports

provides a summary of the IDM reports the system produces.

## 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.




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


**Figure 34: My Reports Window**

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

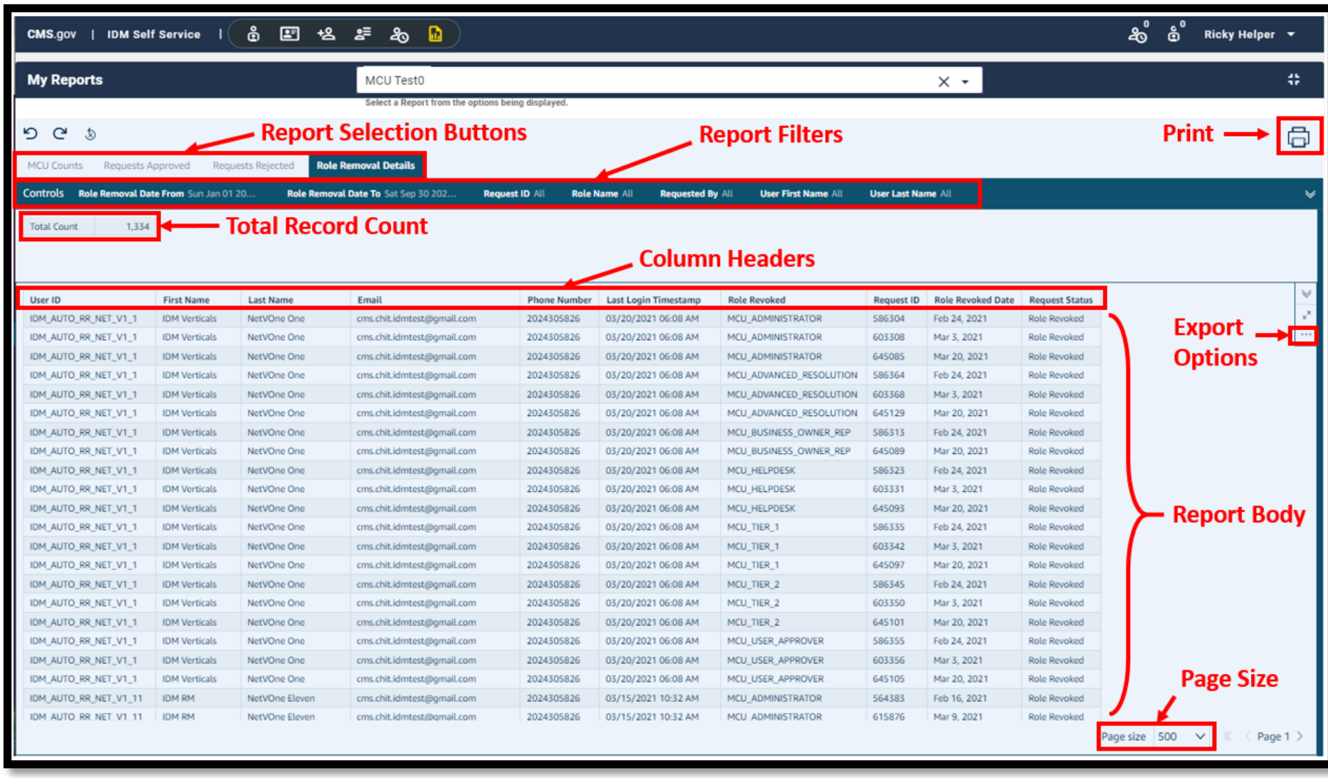
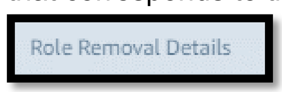
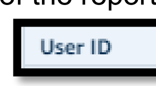



**Figure 35: My Reports Window with Sample Report (Full Screen View)**

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


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


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


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

## How to Print a Report

Use the following procedure to print a report.

1) Select and view the desired report using the procedure in **Section 0 How to Access the IDM Reports**.
2) Select the ***Print*** button and choose the Print option.  The Prepare for printing window opens.
3) Change the ***Paper size*** and/or the ***Paper orientation*** (Optional).
4) Select the ***Print background color*** option if the report title cannot be seen against a white background (Optional).
5) Select the ***Go to preview*** button.
6) Select the ***Print*** button.

## How to Export a Report to an Excel Spreadsheet

1) Select and view the desired report using the procedure in **Section 0 How to Access the IDM Reports**.
2) If the Export Options button is not visible, select on any row of the ***Report Body*** (Optional).

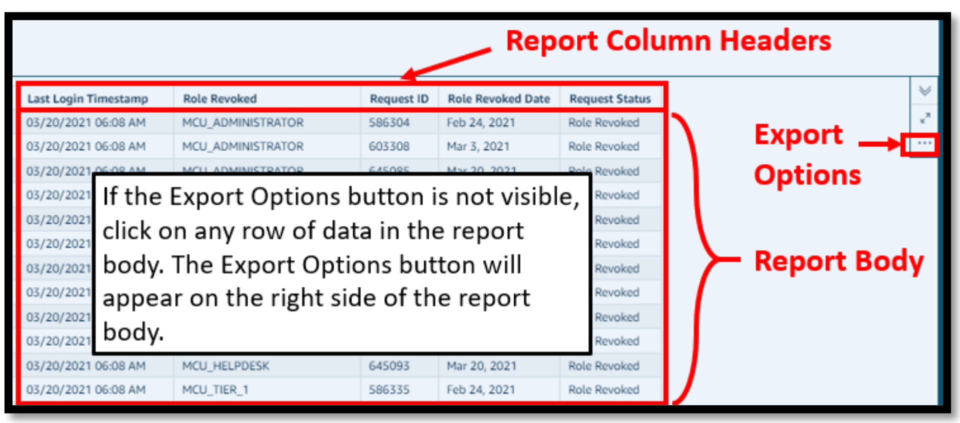
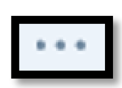



**Figure 36: Location of the My Reports Export Options Button**

3) Select the ***Export Options*** button and select the export format. 
4) The Download Status window appears and displays the progress of the download operation. The Save As window appears after the download is complete.
5) Select the ***Save*** button.
6) Select the ***Done*** button on the Download Status window.

# 15. How to Perform Annual Role Certification

**Note:** The procedures in this section only apply to users who have an Approver role and who certify or revoke roles for other users which fall within the scope of annual role certification.

## Annual Role Certification for Manually Approved Roles

The following terms are introduced in this section:

**Manually Approved Roles -** Roles that are subject to a request and approval process performed by a person. The first or original grant of a manually approved role is valid for one year.

The IDM System sends email reminders to Approvers who manage users with manually approved roles to remind them of the annual role certification date. Email reminders are sent to approvers at intervals of 30, 15, 7, and 1 day(s) before the user's role certification due date.

Business Owners and Business Owner Representatives may also use the "Pending Annual Role Certification" and "Annual Role Certification Summary" reports to obtain information about all user roles that are pending or due for annual role certification. These users must request and be approved for the IDM Reports role before they can access this report. Please refer to **Section 14 How to View IDM Reports** for information on how to view IDM Reports. Additional guidance for accessing and using IDM Reports is contained in the IDM Annual Role Certification Quick Reference Guide.

**Note:** If an approver fails to certify a user's role, the role will be revoked on the certification due date. If a user's role has been revoked, they will have to use IDM's Role Request function as described in **Section 6 How to Request a Role** to request that role again.

### 15.1.1 How to Open and Close the My Annual Role Certifications Function

**Note:** The My Annual Role Certifications button is only available to users who have an Approver role and who certify or revoke manually approved roles.

**Open the My Annual Role Certifications Function:**

1) Select the My Annual Role Certifications button 

located on the Self-Service Dashboard. The My Annual Role Certifications window opens.

**Close the My Annual Role Certifications Function:**

1) Choose one of the following actions to close the My Annual Role Certifications function.
   - Select 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.

## 15.1.2 How to View a List of Pending Certifications

Users view a list of all role certifications that are pending certification or revocation using the My Annual Role Certifications window and the following procedure.

**Note:** The My Annual Role Certifications window displays a list of the first 1000 user roles under an Approver's authority that are pending certification within the next 365 days. A maximum of 1000 roles that are pending certification can be displayed at a time.

1) Select the ***My Annual Role Certifications*** button as described in **Section 0 Annual Role Certification.** The My Annual Role Certifications window appears.

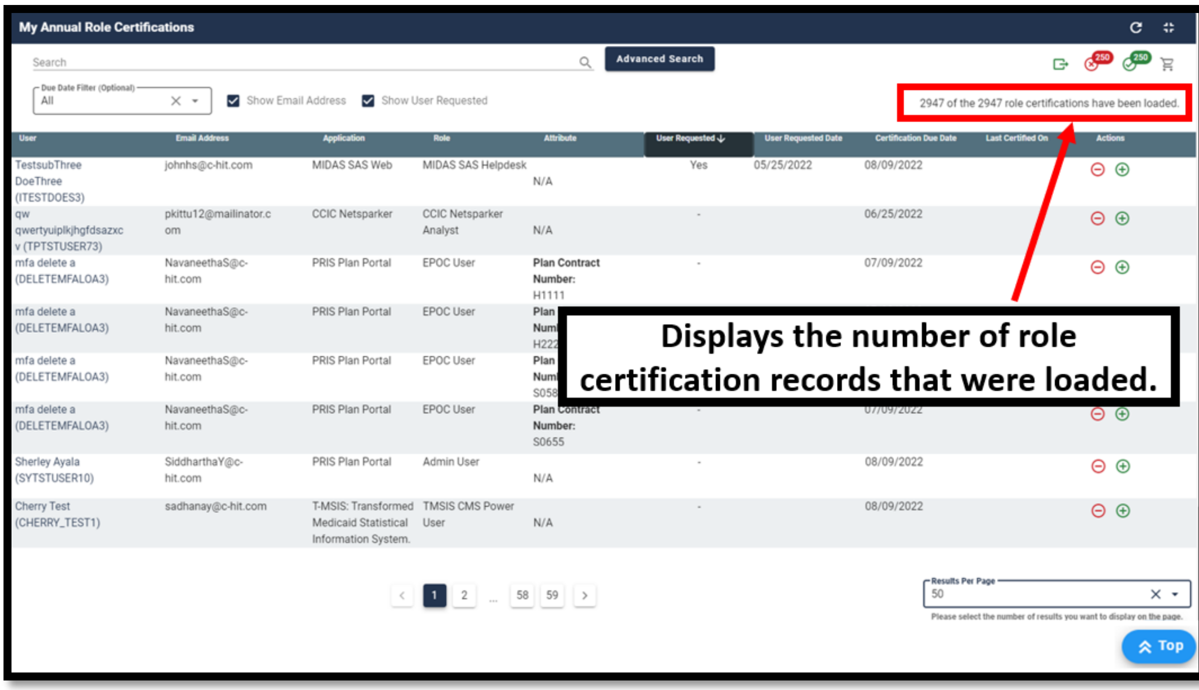
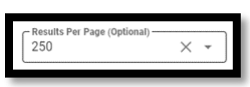



**Figure 37: My Annual Role Certifications Window**

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

3) Use the ***Page Navigation*** controls  to move between pages of results. Select the ***Arrows*** to move to the previous or next page. Select the ***Page Numbers*** to select a specific page of results.

4) Use the ***Due Date*** filter 

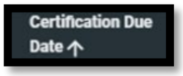
to display only those users whose certifications expire during the desired timeframe (Optional).

5) Select the ***Show Email Address*** filter 

to hide or view the email address column (Optional).

6) Select the ***Show User Requested*** filter 

to hide or view the User Requested and User Requested Date information columns (Optional).

7) Select any ***Column Heading*** 

to sort the list based on the contents of that column (Optional).

### 15.1.3 How to Perform a Global Search

Global Search enables Approvers to perform a keyword search across all information (including role attributes if applicable) to narrow the results of the records in their pending role certification queue.

**Note:** If an Approver has more than 1000 user roles pending role certification, only the first 1000 pending role records can be searched using Global Search.

**Note:** The ***Show Email Address*** box must be selected if you want to perform a Global Search that is based on a user's email address.

Users perform a global search using the following procedure.

1) Select the ***My Annual Role Certifications*** button as described in **Section 0 Annual Role Certification.** The My Annual Role Certifications window appears as illustrated by **Figure 37: My Annual Role Certifications Window**.

2) Enter a keyword into the ***Search*** field. 


3) The screen refreshes and the My Annual Role Certifications window only displays records that contain the global search criteria.

### 15.1.5 How to Perform an Advanced Search

Advanced Search enables Approvers to perform a search using a combination of the following parameters to narrow the results of the records in their pending role certification queue.

- Date range
- Application
- Role
- Group (if applicable)

Approvers can use Advanced Search can be used to certify or revoke users at any time during the year.

Users perform an advanced search using the following procedure.

1) Select the ***My Annual Role Certifications*** button as described in **Section 0 Annual Role Certification.** The My Annual Role Certifications window appears as illustrated by **Figure 37: My Annual Role Certifications Window**.

2) Select the ***Advanced Search*** button. 

The Advanced Search window appears.

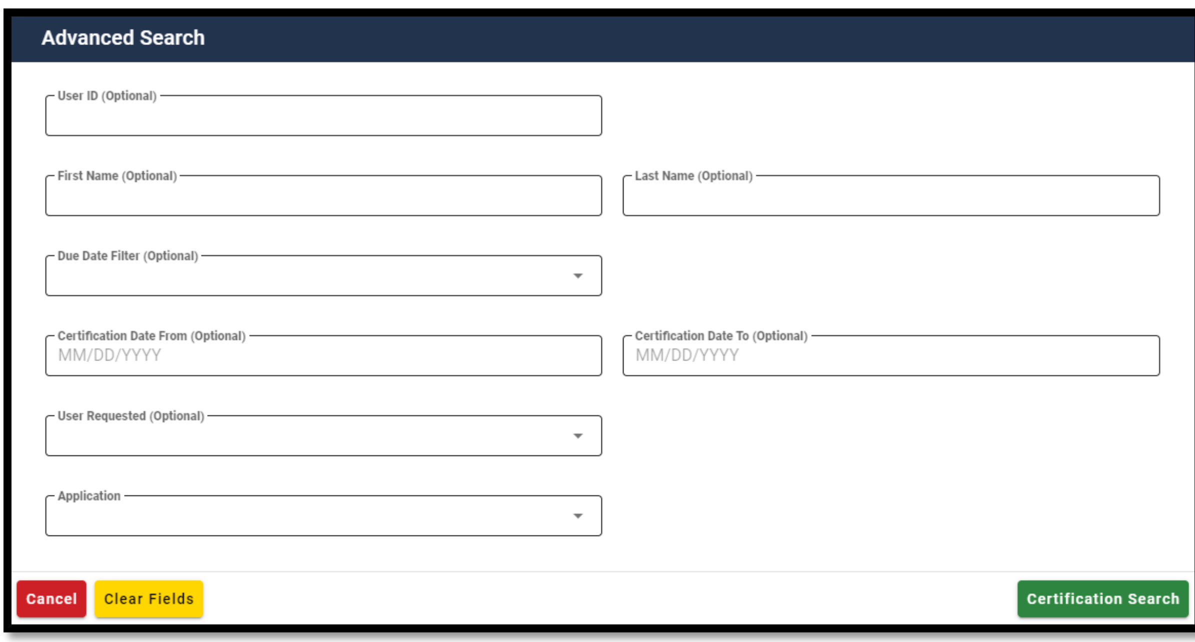



**Figure 38: My Annual Role Certification Advanced Search Window**

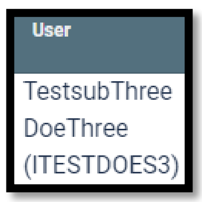
3) Select an Application (Required).
4) Enter any combination of User ID, First Name, Last Name, Certification Date From or Certification Date To (Optional).
5) Select User Requested - (Yes or No) (Optional).
6) Select a Due Date (Optional).

7) Select the ***Certification Search*** button.
8) The screen refreshes and the My Annual Role Certifications window only displays those pending certification records that meet the search criteria.
9) Perform a Global Search by attribute to further narrow the results of an Advanced Search (Optional).

### 15.1.6 How to View User/Role Details and Certify/Revoke a Single User's Role

Approvers have the ability to view a single user's profile information and role details, then certify or revoke that user's role using the following procedure.

**Note:** The Revoke Role function does not immediately remove a user's access to IDM and any application(s). Approvers can immediately remove the user's access via IDM's role removal function.

1) Select the ***My Annual Role Certifications*** button as described in **Section 0 Annual Role Certification.** The My Annual Role Certifications window appears as illustrated by **Figure 37: My Annual Role Certifications** Window.
2) Select the ***User ID*** of the desired user. 

The User Details window appears.

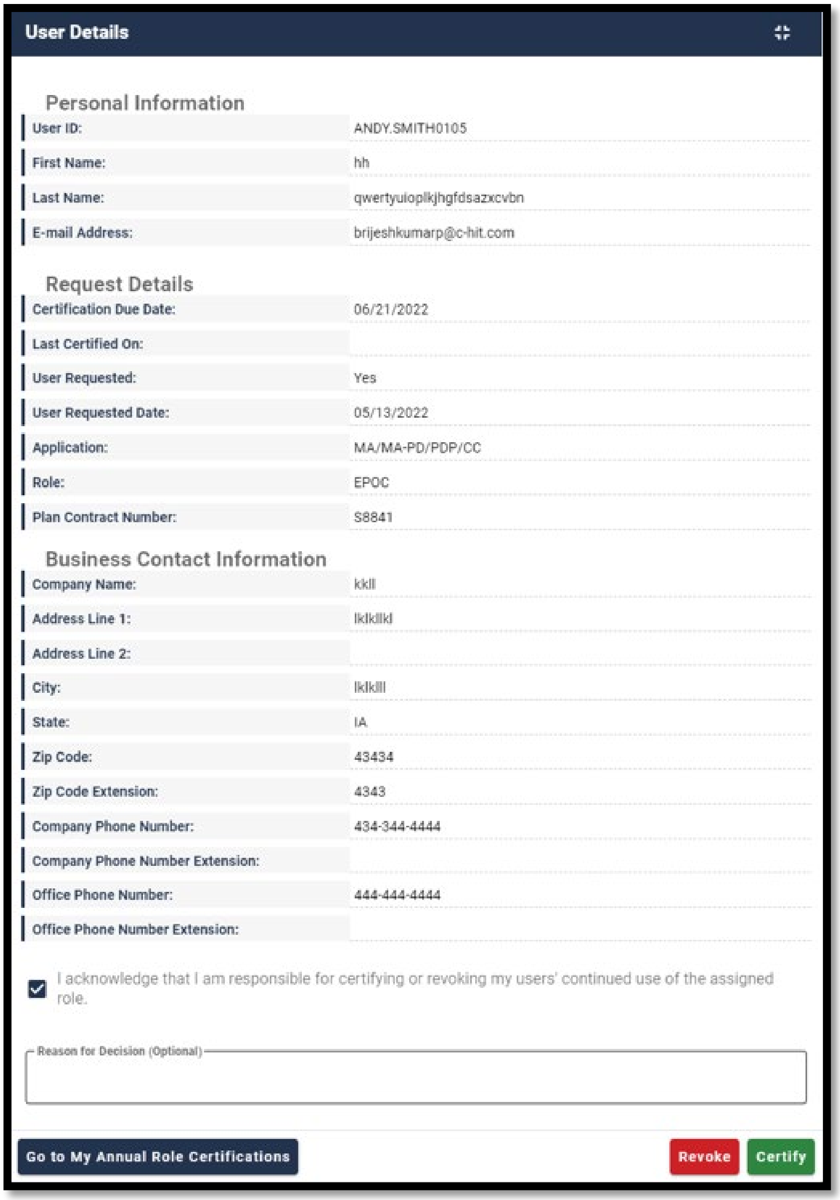



**Figure 39: My Annual Role Certification User Details**

3) Select the ***Acknowledge*** box.
4) Enter a reason for the certify/revoke decision (Optional).
5) Certify or Revoke the user's role.
    a. Select the ***Certify*** button to certify the user's role.
    Or
    b. Select the ***Revoke*** button to revoke the user's role.
6) The system displays a message that states the transaction was successful.

### 15.1.7 How to Bulk Certify or Revoke Multiple User Roles

The Bulk Certify/Revoke feature enables Approvers to select all user roles that are displayed on the current page of results then bulk-submit them for certification or revocation. A maximum of 1000 roles that are pending certification can be certified or revoked in a single transaction.

> Warning: The more role certifications you process in one transaction, the longer it will take for that transaction to complete. A maximum of 500 roles per transaction is recommended.

1) Select the ***My Annual Role Certifications*** button as described in **Section 0 Annual Role Certification.** The **My Annual Role Certifications** window appears as illustrated by **Figure 37: My Annual Role Certifications Window**.

2) Use the ***Pagination*** control 

to adjust the number of pending certification records that are displayed on each page (Optional).

3) Use the ***Due Date*** filter 

to display only those users whose certifications expire during the desired timeframe (Optional).

4) Certify or Revoke the user's role.

   a. Select the ***Certify all*** button 

flag all roles displayed on the page for certification.

      Or

   b. Select the ***Revoke all*** button 

to flag all roles displayed on the page for revocation.

6) The Certification(s) to process window appears.

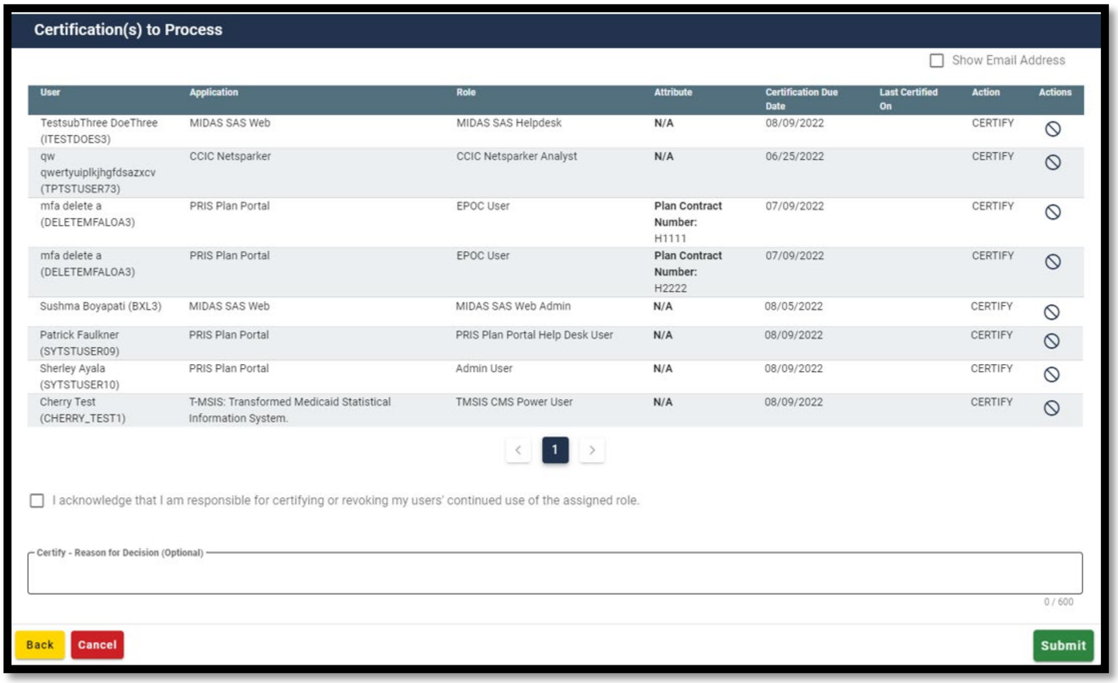



**Figure 40: Certifications to Process Window**

7) Select the ***Remove from Cart*** button  to reverse the certify or revoke action for a single role (Optional).

8) Select the ***Acknowledge*** box.

9) Enter a reason for the certify/revoke decision (Optional).

10) Select the ***Submit*** button. All flagged roles are certified or revoked

11) The system displays a message that states the transaction was successful.

### 15.1.8 How to use the Cart to Certify and Revoke Multiple User Roles

The Cart enables Approvers to select multiple user roles then certify and revoke those roles simultaneously in one transaction. A maximum of 1000 roles that are pending certification can be certified or revoked in a single transaction using the Cart.

> Warning: The more role certifications you process in one transaction, the longer it will take for that transaction to complete. A maximum of 500 roles per transaction is recommended.

1) Select the ***My Annual Role Certifications*** button as described in **Section 0 Annual Role Certification.** The **My Annual Role Certifications** window appears as illustrated by Figure 37: My Annual Role **Certifications** Window.

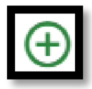
2) Use the ***Pagination*** control 

to adjust the number of pending certification records that are displayed on each page (Optional).

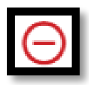
3) Use the ***Due Date*** filter 

to display only those users whose certifications expire during the desired timeframe (Optional).

4) Certify or Revoke the user's role.

   a. Select the ***Certify*** button.  The record turns green and is flagged for certification in the Cart. The Cart's counter increases by one for each flagged record.

   Or

   b. Select the ***Revoke*** button.  The record turns red and is flagged for revocation in the Cart. The Cart's counter increases by one for each flagged record.

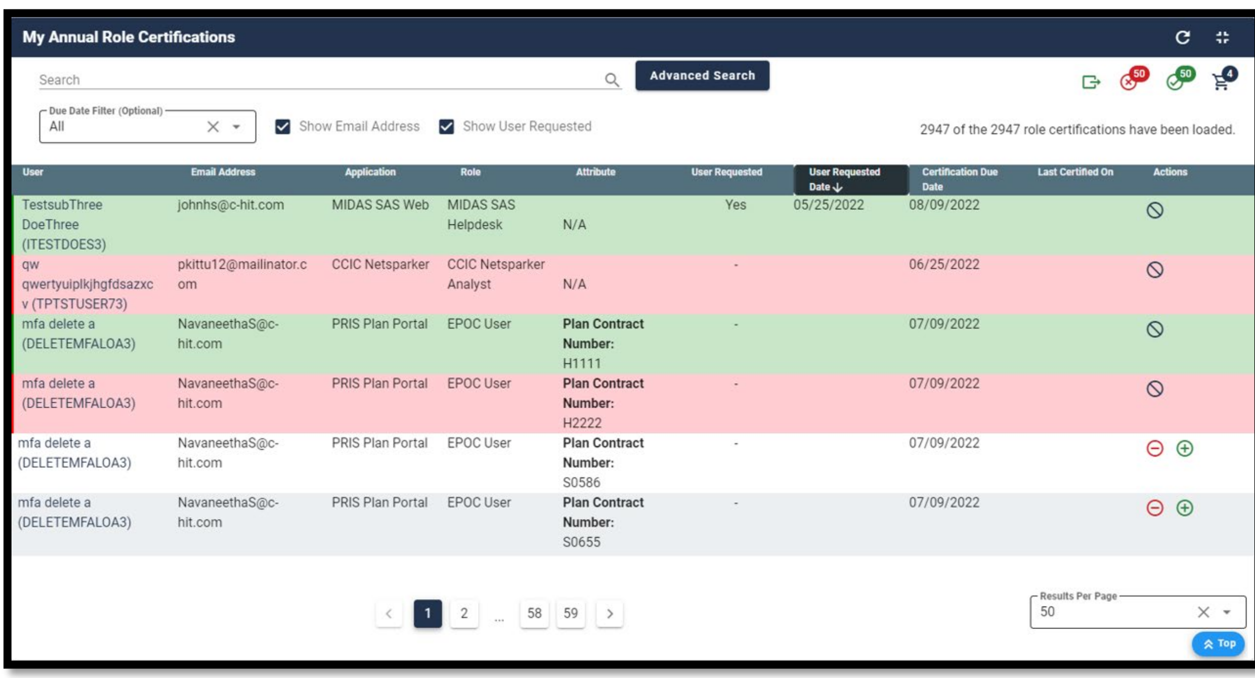



**Figure 41: Certify and Revoke Multiple User Roles using the Cart Feature**

5) Select the ***Remove from Cart*** button  to reverse the certify or revoke action for a single role. The Cart's counter decreases by one for each record that is removed (Optional).

6) Select the ***Cart*** button  . The **Certification(s) to Process** window appears as illustrated by **Figure 40: Certifications to Process Window**.
7) Select the ***Acknowledge*** box.
8) Enter a reason for the certify/revoke decision (Optional).
9) Select the ***Submit*** button. The system displays a message that states the action was successful.

## Annual Role Certification for Programmatically Approved Roles

The following terms are introduced in this section:

**Programmatically Approved Roles -** Roles that are subject to an automated validation check where user provided data is programmatically compared to data maintained in a trusted source. These roles have an annual role certification due date of June $1^{st}$ each year.

**Note:** This section only applies to Approvers and Business Owners of applications that manage users who have programmatically approved roles. The Connexion application is currently the only IDM integrated application that uses programmatically approved roles.

The IDM System performs an Annual Role Certification pre-check validation of user roles based on a comparison of information the user provided during the initial role request and information that is maintained in a trusted source. User roles that pass this pre-check are automatically recertified by the system on June $1^{st}$ annually.  Approvers are not required to take any action.

### 15.1.9 System Notifications Sent for Users who Fail Pre-check Validation

The IDM System sends email notifications to next level application Approvers and Business Owners with information about users who fail the pre-check validation. This email includes the user's role details and directs the next level application Approvers and Business Owners to take action to correct any discrepancies before the June $1^{st}$ certification due date for programmatically approved roles.

The initial email is sent 90 days before the June $1^{st}$ certification due date. Subsequent reminder emails are sent at 60 days, 30 days, 7 days, and 1 day before the June $1^{st}$ certification due date if the discrepancies are not corrected.

**Note:** If the next level application Approver or Business Owner fails to correct the discrepancies before the June $1^{st}$ role validation check, the affected users will fail Annual Role Certification and their roles will be automatically revoked. Any user whose role has been revoked, will have to request that role again by using the IDM's Role Request function as described in **Section 6 How to Request a Role**.

Approvers may also use the "Pending Annual Role Certification" report to obtain information about all user roles that are pending or due for annual role certification. Approvers must request and be approved for the IDM Reports role before they can access this report. Please refer to **Section 14 How to View IDM Reports** for information on how to view IDM Reports.

# 16. Instructions for Help Desks

## 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:

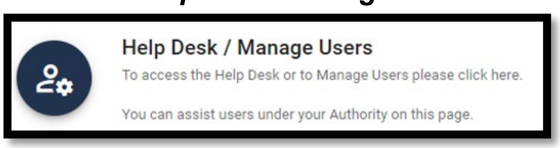
- Perform an Application Search (Tier 1 only)
- Perform an Enterprise Search
- Suspend a user’s account
- Remove a user’s roles
- Cancel a user’s pending requests
- Reset a user’s password
- Unlock a user’s account
- Manage a user’s IAL
- Unsuspend a user’s account (Tier 2 only)
- Create User Audit reports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

## 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:**

Select the ***Help Desk/Manage Users*** button located on the Self-Service Dashboard.




The Application Search window appears.

## How to Choose the Appropriate Search

The matrix illustrated by **Figure 42: 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 42: Application and Enterprise Search Capabilities Matrix**

## 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) Select the ***Help Desk/Manage Users*** button. The Application Search form appears.

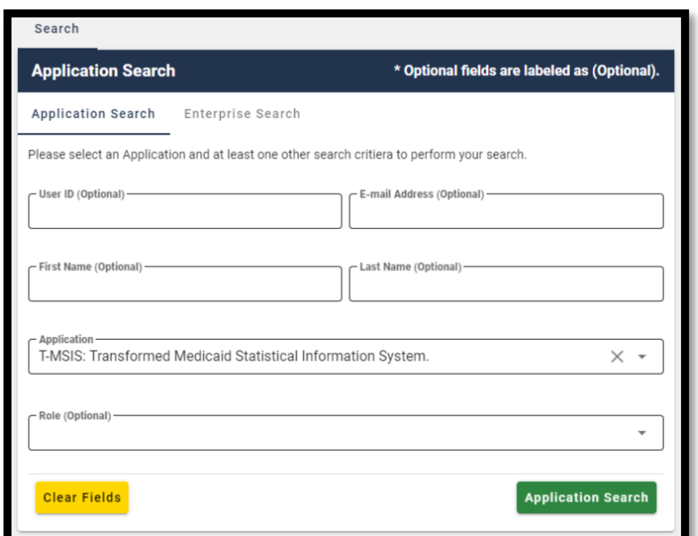



**Figure 43: Help Desk Application Search Form**

2) Select an application from the ***Application*** list. The Role list appears.
3) Select a role from the ***Role*** list. Selecting a Role will limit the search to users who possess that role within the application (Optional).
4) 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 (Optional).
5) Select 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.

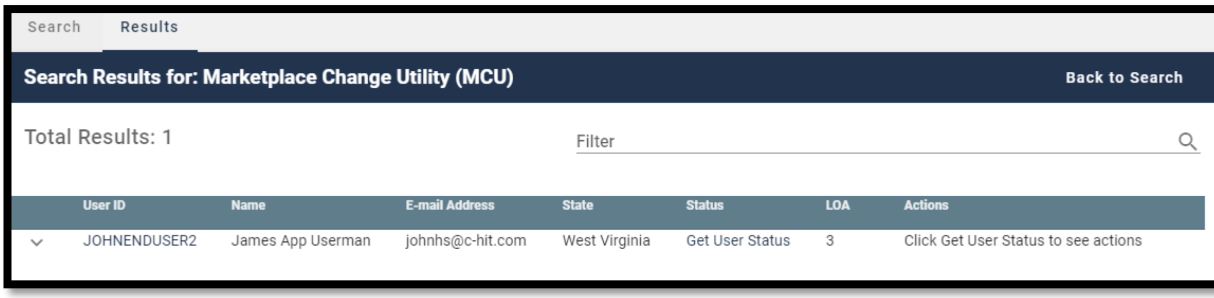



**Figure 44: Help Desk Application Search Results**

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

## 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) Select 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) Select the ***Enterprise Search*** button.


The Enterprise Search Form appears.

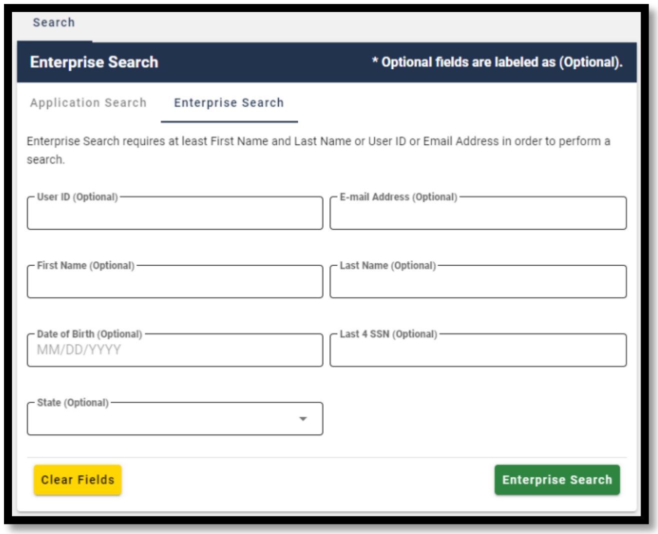



**Figure 45: Help Desk Enterprise Search Form**

3) Enter any combination of User ID <u>or</u> Email Address <u>or</u> First Name <u>and</u> *Last Name*.
4) 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 (Optional).
5) 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 (Optional) Select.
6) Select the ***Enterprise Search*** button. The screen refreshes and the search results appear.

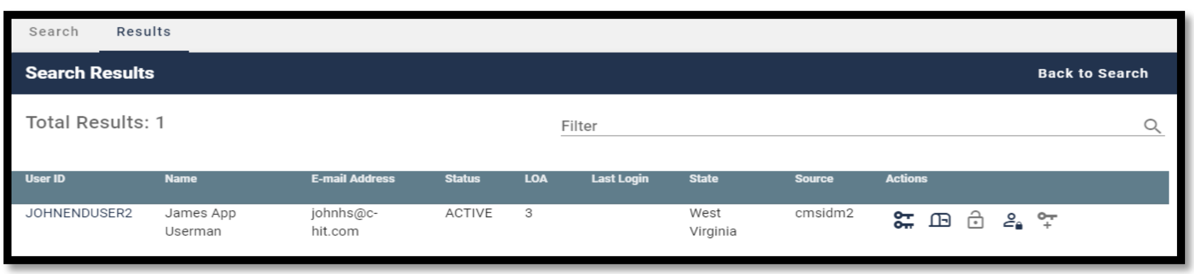



**Figure 46: Help Desk Enterprise Search Results**

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

## 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) According to the procedures in **Section 0 "How to Perform an Application Search"** and **"How to Perform an Enterprise Search"**, perform an Application Search or an Enterprise Search. The screen refreshes and the search results appear.

2) Select the ***User ID*** 

for the desired user. The screen refreshes, the User Details window appears and displays the User Profile information.

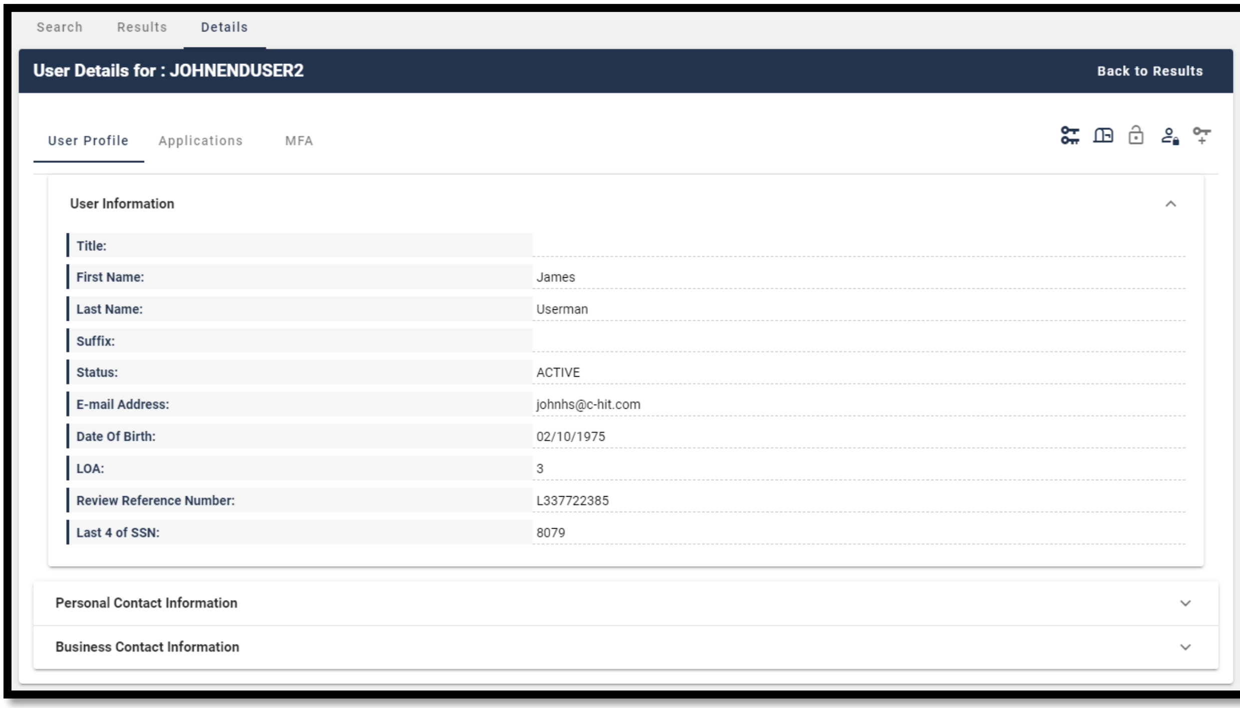
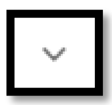



**Figure 47: User Details User Profile Tab**

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

## How to View a Summary of a User's Applications

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

1) According to the procedures in **Section 0 "How to Perform an Application Search"** and **"How to Perform an Enterprise Search"**, perform an Application Search or an Enterprise Search. The screen refreshes and the search results appear.

2) Select the ***User ID*** 

for the desired user. The screen refreshes, the User Details window appears and displays User Profile information.

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

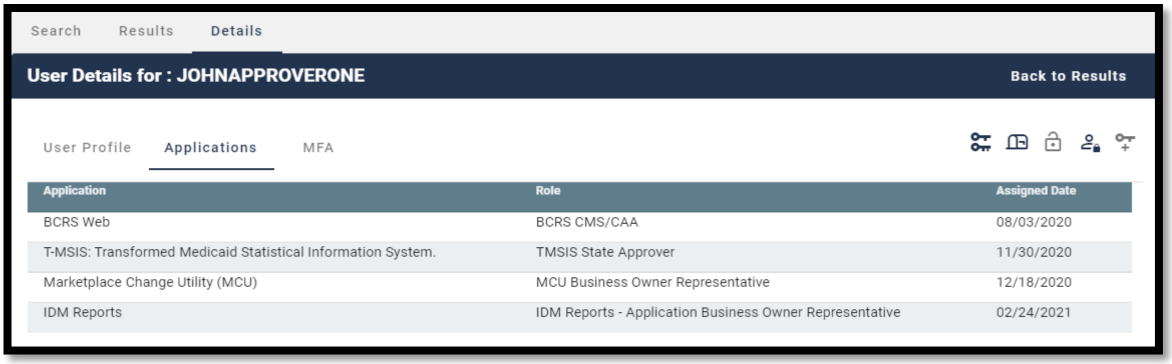
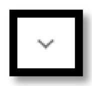



**Figure 48: Enterprise Search Results - Applications Tab**


**Figure 49: Application Search Results - Applications Tab**

4) (If applicable) Select the ***Expand Detail*** button.  A summary of role information for the desired application appears. [30]

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

## 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.

[30] 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.

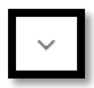
> **Note:** The IDM System will display a warning message if the role removal or attribute removal operation will remove the last approver of an organization that still has users associated with that role or attribute. Such users could be left in an "orphaned" state without an approver of record for 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 0 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. Select 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.

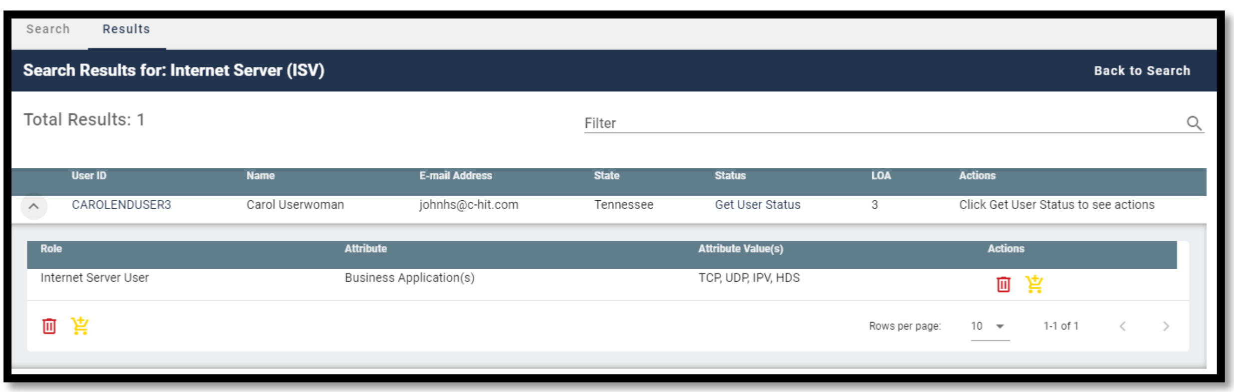
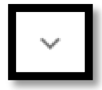



**Figure 50: Application Search Results**

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

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

B. Select the ***Applications*** tab. A summary of the user's applications appears.

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

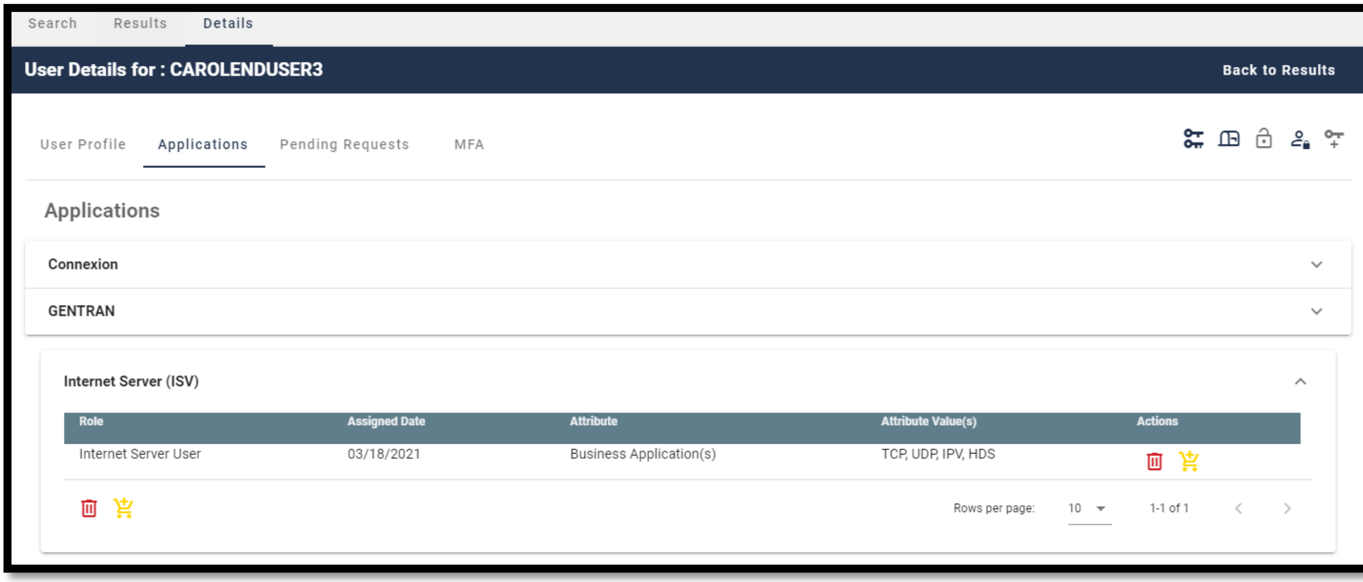
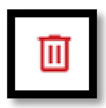



**Figure 51: User Details Applications Tab**

3) Select the ***Remove Now*** button  for the role that requires removal. The Remove Role/Attribute window appears.
4) Enter a justification and select 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. [31]

---

[31] 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.

## 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.

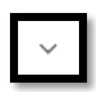
**Note:** The IDM System will display a warning message if the role removal or attribute removal operation will remove the last approver of an organization that still has users associated with that role or attribute. Such users could be left in an “orphaned” state without an approver of record for future 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 0 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 52: List of User’s Roles / Attributes**.

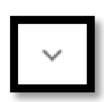
2a) **This option uses the Search Results window**.

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

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

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

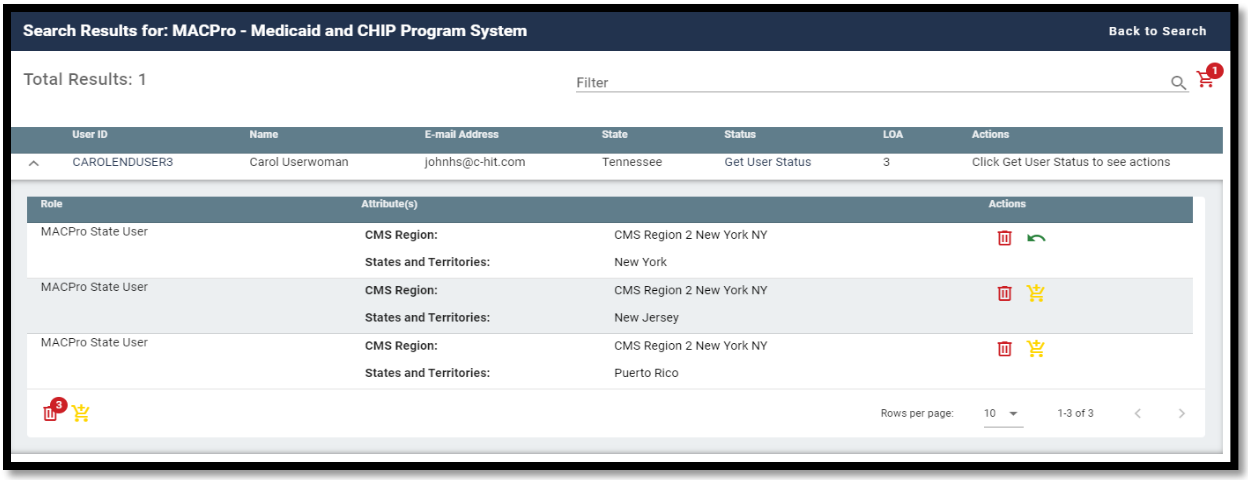



**Figure 52: List of User's Roles / Attributes**

3) Select the ***Add to Cart*** button  for the individual role that requires removal. The ***Remove From Cart*** button appears.[32]

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

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.

---

[32] Select 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(Optional).

6) Select the ***Remove All Now*** button. 

The Remove Role/Attribute window appears.[33]

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

8) Enter a justification and select 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.[34]

## 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 0 How to Perform an Application Search.**

2) Select the ***User ID*** 

for the desired user. The screen refreshes, the User Details window appears and displays User Profile information.

3) Select the ***Pending Requests*** tab. 

A list of the user's pending requests appears.

[33] Select the ***Remove All Now*** button 

located at the bottom left of the window to remove all roles displayed on the current page (Optional).

[34] 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.

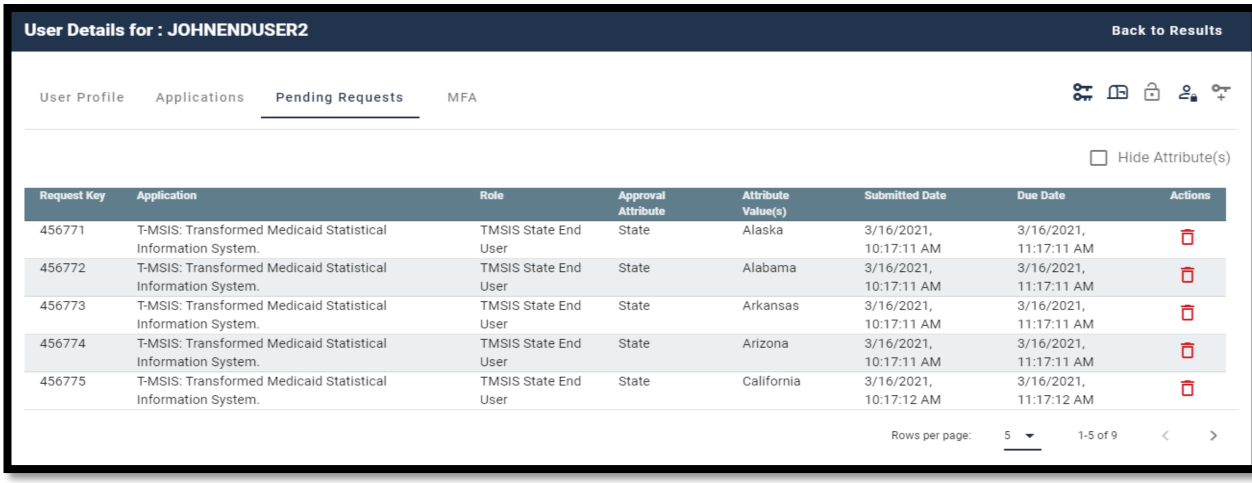



**Figure 53: User Details Pending Requests Tab**

4) Select 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 select 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. [35]

## 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, IVR, 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.

[35] 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.
- **Actions** - A button for the action that can be performed on the device.

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

1) Perform an Application Search according to the procedure in **Section 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.
2) Select the ***User ID*** for the desired user. The User Details window appears and displays the User Profile information.
3) Select the ***MFA*** tab. 

The MFA device summary appears.

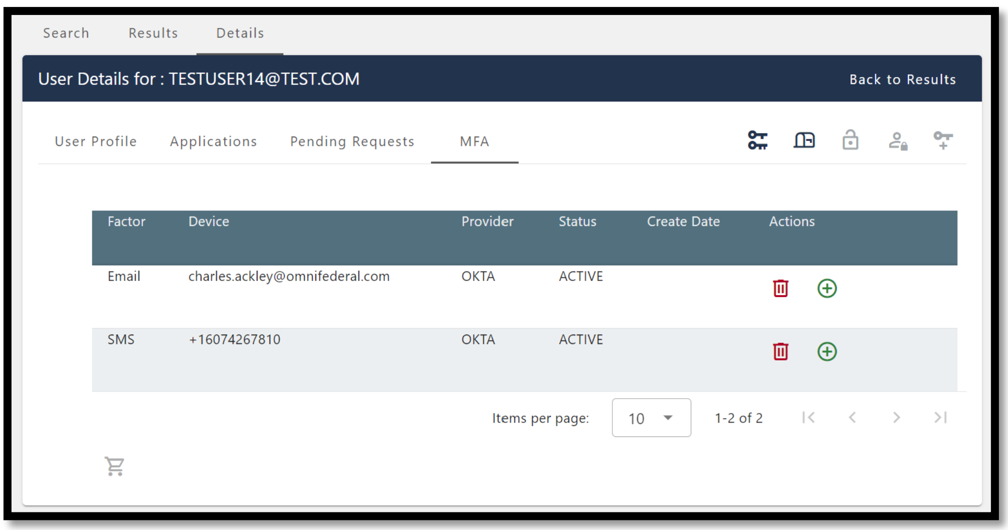



**Figure 54: User Details MFA Device Summary**

### 16.1.1 How to Remove Individual MFA Devices

Help Desk Users have the capability to remove individual MFA devices from a user's account.

**Note:** A Tier 1 or Tier 2 Help Desk User may remove all of the given user's MFA devices except email (email MFA can be updated, not removed)

**Note:** Tier 1 and Tier 2 Help Desk Users cannot add an MFA device for an end user.

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

1) Perform an Application Search according to the procedure in **Section 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.
2) Select the ***User ID*** for the desired user. The User Details window appears and displays the User Profile information.
3) Select the ***MFA*** tab. 

The MFA device summary appears as illustrated by **Figure 54: User Details MFA Device Summary.**
4) Select the Remove Factor button.  The Remove MFA Device window appears.
5) Enter a justification and select the ***Remove MFA Device*** button. The Help Desk UI displays a message that indicates the MFA device was successfully removed.[36]

### 16.1.2 How to Remove Multiple MFA Devices Simultaneously

Help Desk Users have the capability to remove multiple MFA devices from a user's account simultaneously.

**Note:** A Tier 1 or Tier 2 Help Desk User may remove all of user's MFA devices, but that user will be prompted to set up MFA the next time they sign in.

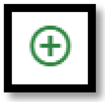
The following procedure provides the steps to view a user's MFA devices using the Help Desk UI ***MFA*** tab.

1) Perform an Application Search according to the procedure in **Section 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.
2) Select the ***User ID*** for the desired user. The User Details window appears and displays the User Profile information.
3) Select the ***MFA*** tab. 

The MFA device summary appears as illustrated by **Figure 54: User Details MFA Device Summary.**

[36] The system sends an email to the affected user's email address on record which indicates that an MFA device on their account has been reset. It also indicates where the user can obtain assistance if they have questions.

4) This option permits the **Help Desk User** to select specific **MFA** devices to remove simultaneously**.**

A. Choose which devices to remove: Select the ***Add to Cart*** button  to add a specific MFA device to the Cart for removal. The Cart counter increments for each device that is added to the Cart.

B. (Optional) Select the ***Remove From Cart*** button  to remove a specific MFA device from the Cart. The Cart counter decreases for each device that is removed from the Cart.

C. Select the ***Process Requests*** button. 

The Remove MFA Device window appears.

5) Enter a justification and select the ***Remove MFA Device(s)*** button. The Help Desk UI displays a message that indicates the MFA device was successfully removed. [37]

## 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 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.

[37] The system sends an email for each MFA device that was removed to the affected user's email address on record which indicates that an MFA device on their account has been reset. It also indicates where the user can obtain assistance if they have questions.

2) (Application Search Users Only) Select the ***Get User Status*** button.


The Update E-mail Address button appears under the “Actions” column.

3) Select 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 select the ***Submit*** button. The system displays a message that indicates the operation completed successfully.

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

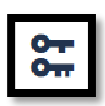
When a user is unable to reset their password using the IDM System Self-Service Dashboard, that user may request the assistance of a Help Desk User. The Help Desk user initiates a password change operation by sending a Password Reset email to the requesting user. The email is sent to the email address 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 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.
2) (Application Search Users Only) Select the ***Get User Status*** button.


The ***Reset Password*** button appears under the “Actions” column.

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

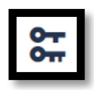
5) Select the ***Submit*** button. The system displays a message which indicates the operation completed successfully.[38] [39]

## 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 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.
2) (Application Search Users Only) Select the ***Get User Status*** button. 

The ***Reset Password*** button appears under the “Actions” column.
3) Select the ***Reset Password*** button  for the desired user. The Reset Password window appears.
4) Select the “***Display a temporary password on-screen***” option and enter a justification.
5) Select the ***Submit*** button. The Reset Password window refreshes and displays a temporary password.
6) Provide the temporary password to the user.[40]
7) Select the ***Close*** button. The system displays a message which indicates the operation completed successfully.[41] [42]

---

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

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

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

[41] 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.

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

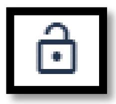
## How to Unlock a User's Account

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 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 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) Select the ***Get User Status*** button. The ***Unlock Account*** button appears under the "Actions" column.
3) Select the ***Unlock Account*** button  for the desired user. The Unlock Account window appears.
4) Enter a justification and select the ***Submit*** button. The system displays a message that indicates the operation completed successfully.

## 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.

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 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears.


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

3) Select the ***Suspend Account*** button  for the desired user. The Suspend Account window appears.
4) Select the "***I confirm that I want to Suspend the User's Account***" option.
5) Enter a justification and select the ***Submit*** button. The system displays a message that indicates the user's account is suspended.[43] [44]

[43] 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.

[44] 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.

# 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.

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 0 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 0 How to Perform an Enterprise Search**. The Search Results window appears. [45]


2) (Application Search Users Only) Select the ***Get User Status*** Button. The ***Update LOA*** button appears under the “Actions” column.

3) Select 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. [46]

5) Use the ***LOA*** menu to select the updated LOA. [47]

---

[45] 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**.

[46] 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.

[47] A user’s LOA can only be raised; it cannot be lowered.

6) Use the ***LOA Reason*** menu to select the reason for the LOA update action.
7) Enter a justification and select the ***Submit*** button. the system displays a message that indicates the operation completed successfully.

## 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.

1) Perform an Enterprise Search according to the procedure in **Section 0 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) Select the ***Unsuspend Account*** button  for the suspended user. The Unsuspend Account window appears.
3) Enter a justification and select the ***Submit*** button. The system displays a message that indicates the user's account is now unsuspended.

## 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) Select the ***Help Desk/Manage Users*** button as described in **Section 0 How to Access the Help Desk Functions.** The Enterprise Search form appears.

2) Select the ***User Audit*** button. 

The User Audit Search form appears.

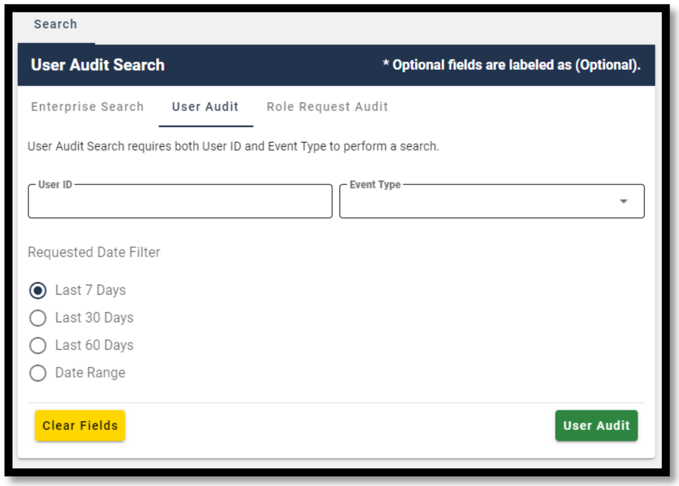
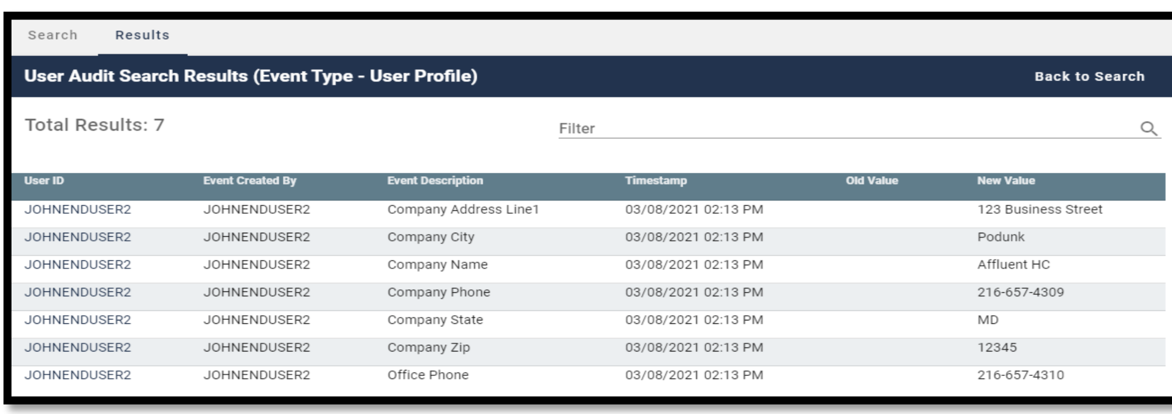



**Figure 55: Help Desk User Audit Search Form**

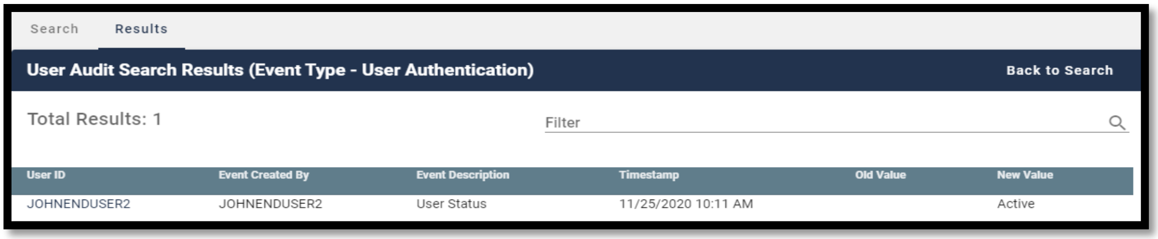
3) Enter a User ID.
4) Select an Event Type from the list.
5) Select a Date Range.
6) Select the ***User Audit*** button. 

The screen refreshes and the report appears on the Results tab.




| 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 56: User Audit Report - User Profile Events**



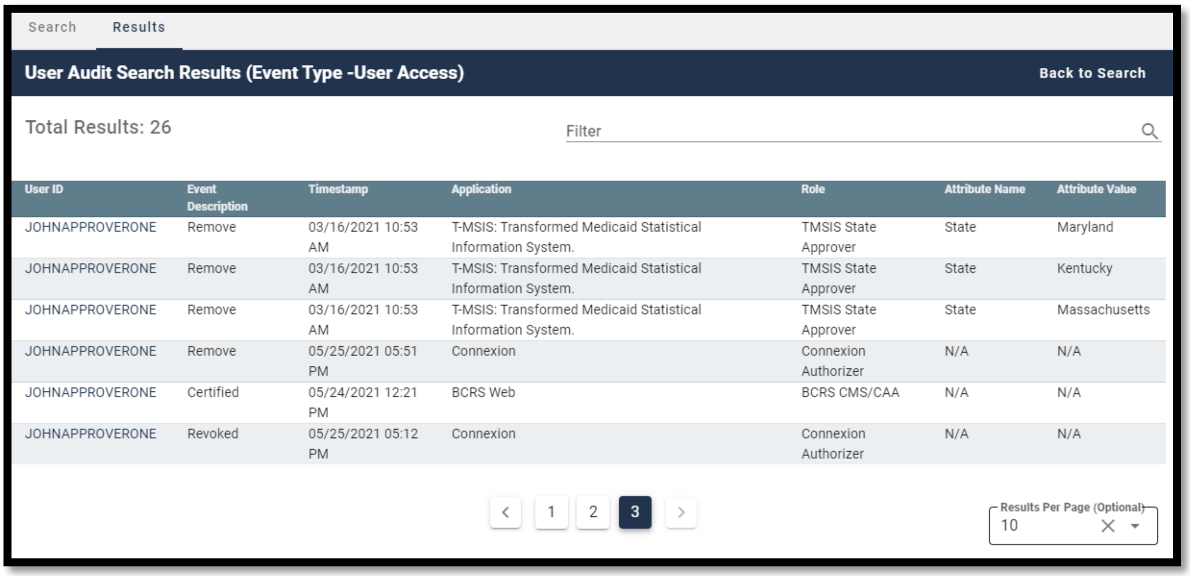
Search Results

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 57: User Audit Report - User Authentication Events**



Search Results

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

Total Results: 26 Filter

| User ID | Event Description | Timestamp | Application | Role | Attribute Name | Attribute Value |
|---|---|---|---|---|---|---|
| JOHNAPPROVERONE | Remove | 03/16/2021 10:53 AM | T-MSIS: Transformed Medicaid Statistical Information System. | TMSIS State Approver | State | Maryland |
| JOHNAPPROVERONE | Remove | 03/16/2021 10:53 AM | T-MSIS: Transformed Medicaid Statistical Information System. | TMSIS State Approver | State | Kentucky |
| JOHNAPPROVERONE | Remove | 03/16/2021 10:53 AM | T-MSIS: Transformed Medicaid Statistical Information System. | TMSIS State Approver | State | Massachusetts |
| JOHNAPPROVERONE | Remove | 05/25/2021 05:51 PM | Connexion | Connexion Authorizer | N/A | N/A |
| JOHNAPPROVERONE | Certified | 05/24/2021 12:21 PM | BCRS Web | BCRS CMS/CAA | N/A | N/A |
| JOHNAPPROVERONE | Revoked | 05/25/2021 05:12 PM | Connexion | Connexion Authorizer | N/A | N/A |

1 2 3

Results Per Page (Optional) 10

**Figure 58: User Audit Report - User Access Events**

7) (Optional) Select the ***User ID*** button 

for the desired event. The Role Audit Details window appears and displays role details for the selected event.

8) Select the ***Back to Results*** button. 

The search results window appears.

## 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) Select the ***Help Desk/Manage Users*** button as described in **Section 0 How to Access the Help Desk Functions.** The Enterprise Search form appears.

2) Select the ***Role Request Audit*** button. 

The Role Request Audit Search form appears.

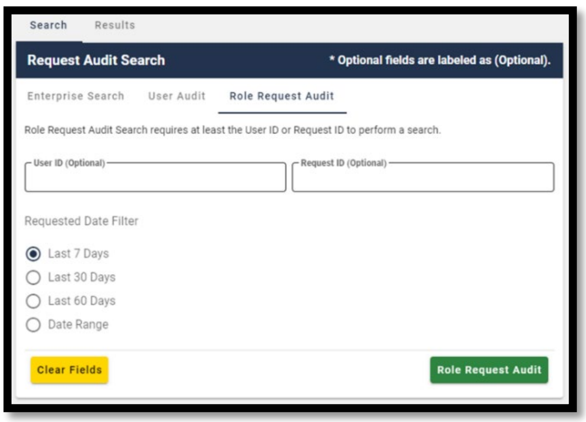
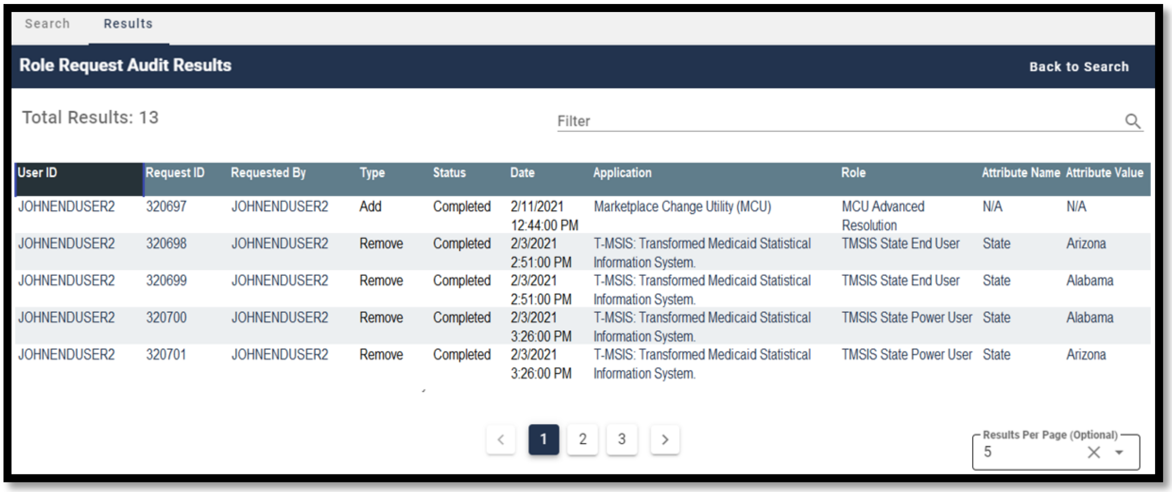



**Figure 59: Help Desk Role Request Audit Search Form**

3) Enter a User ID or enter a Request ID.
4) Select a Date Range.
5) Select the ***Role Request Audit*** button. 

The screen refreshes and the report appears on the Results tab.




| 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 60: Role Request Audit Report**

6) (Optional) Select the ***User ID*** button 

for the desired event. The Role Audit Details window appears and displays role details for the selected event.

7) Select the ***Back to Results*** button. 

The search results window appears.

## 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.[48]

1) The Application Team/Owner creates the YubiKey Seed File using the procedure outlined in **Section 16.1.3 How to Generate the YubiKey Seed File**
2) The Application Team/Owner creates an IDM Service Request (SR) and attaches the YubiKey Seed File.[49]
3) The IDM SR Team processes the IDM SR and hands it off to the IDM Okta Team.

---

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

[49] 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

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 0 How to Add a YubiKey MFA Device**. [50]

**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 16.1.5 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.

### 16.1.3 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. [51]

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

[50] 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.

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

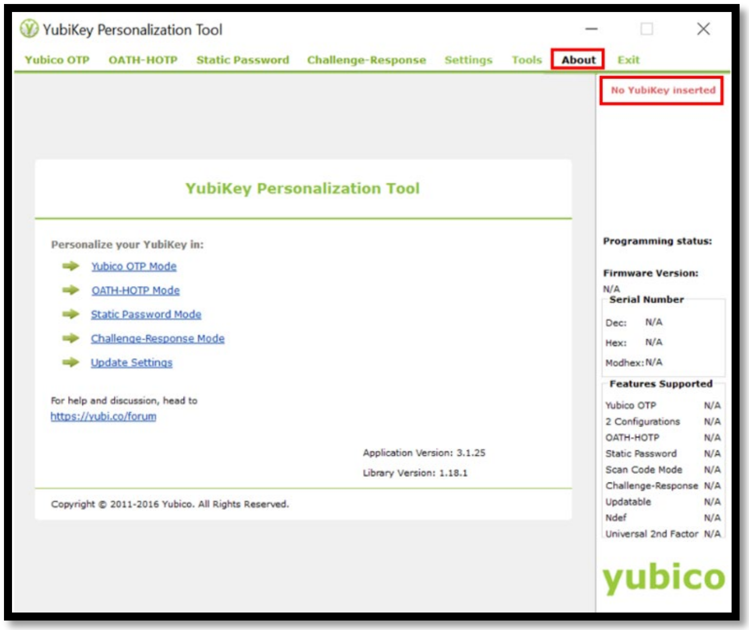



**Figure 61: YubiKey Personalization Tool Startup Window**

2) Select 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.

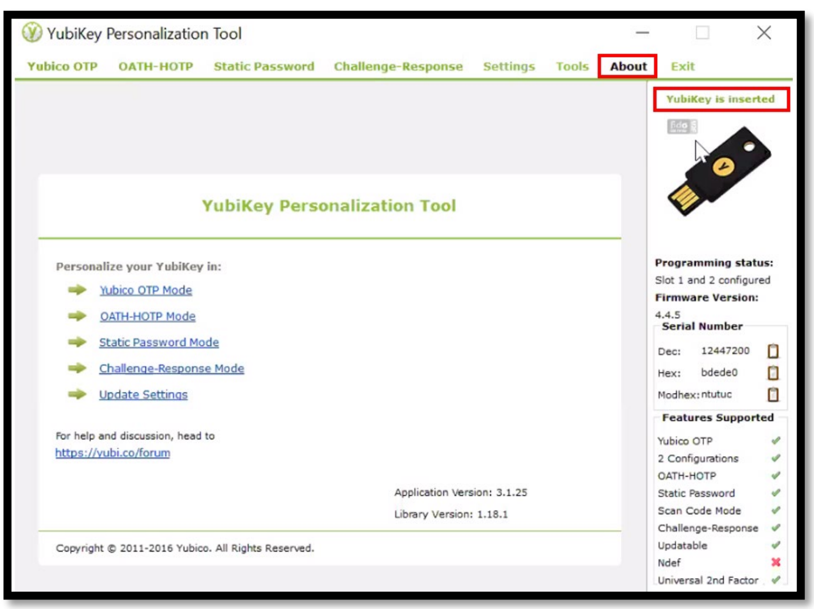



**Figure 62: YubiKey Personalization Tool - Device Present**

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

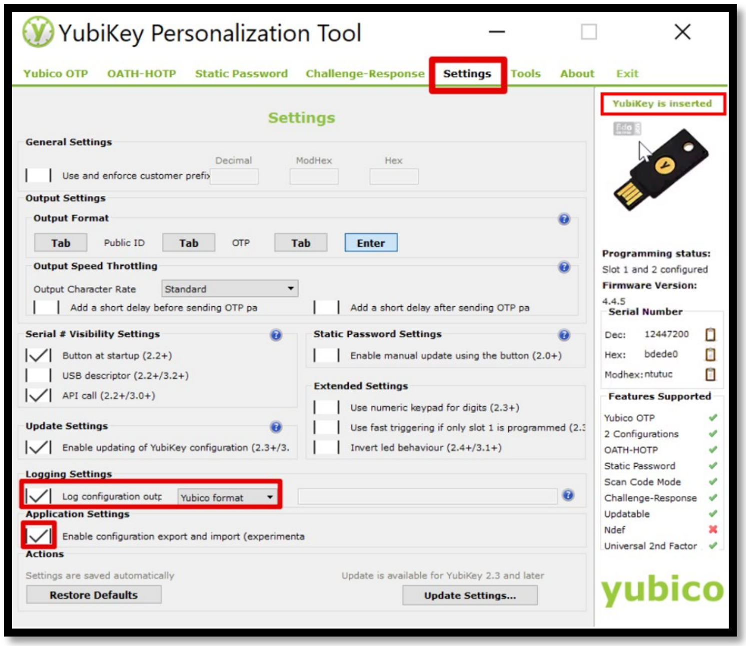



Figure 63: YubiKey Personalization Tool - Settings Tab

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

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

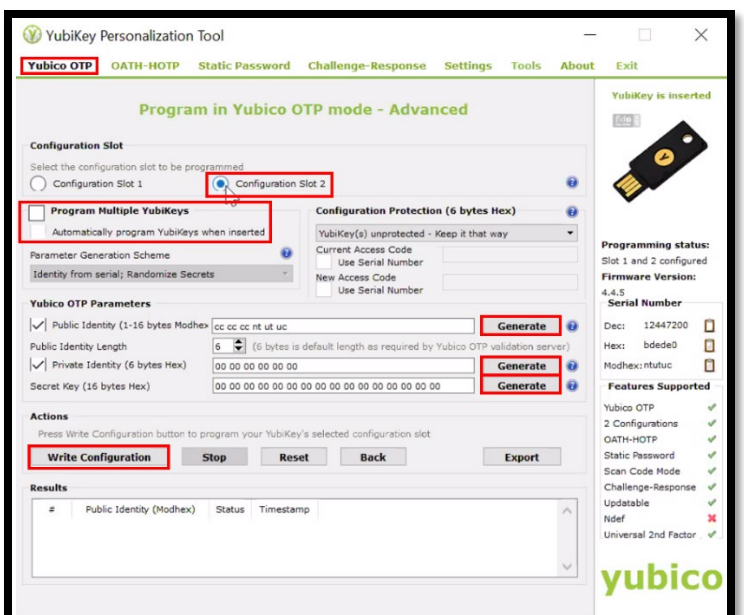



Figure 64: YubiKey Personalization Tool - Yubico OTP Tab

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

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

11) 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 (Optional).

12) Select 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.

### 16.1.4 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) Select the ***Security*** menu option.

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

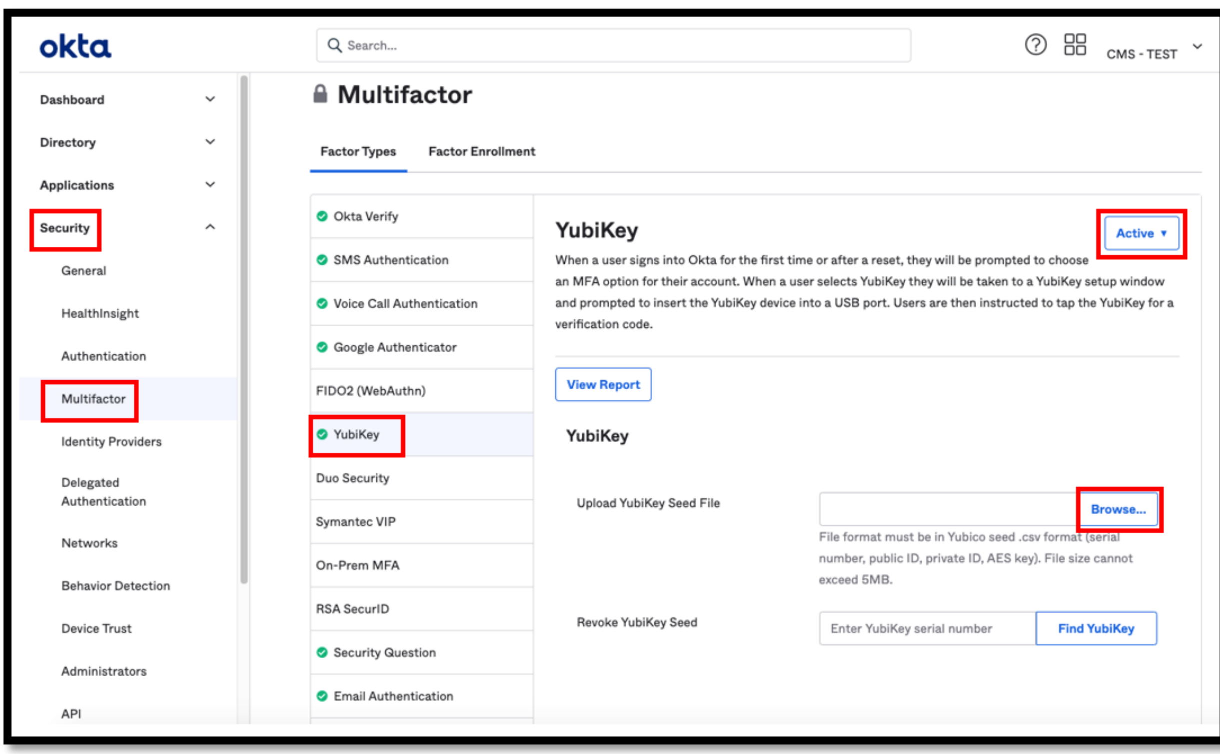



**Figure 65: Okta YubiKey Administration Window**

4) 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** (Optional).
5) Select 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. |

### 16.1.5 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) Select the ***Security*** menu option.
3) Select the ***Multifactor*** menu option, then select ***YubiKey***. The YubiKey administration window appears as illustrated by **Figure 65: Okta YubiKey Administration Window**.
4) Select the ***View Report*** button and obtain the serial number of they YubiKey that will be revoked (Optional).
5) Enter the YubiKey serial number into the ***Revoke YubiKey Seed*** field then select 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) Select 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 15 characters in length.
- Passwords must include an uppercase letter.
- Passwords must include a lowercase letter
- Passwords must include a number (0 - 9).
- Passwords must not contain a space.
- Passwords must not be one of the user's last 6 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: Summary of IDM Reports

My Reports provides approved users with the ability to view one or more types of IDM reports that assist those users with the task of effectively managing other users who are under their authority.

**Table 4: Summary of Current IDM Reports** provides a summary of the reports that are available to users with Business Owner, Business Owner Representative, or Tier 1 Application Help Desk roles who have also been approved for the IDM Reports role as of the date this user guide was released. [52]

**Table 4: Summary of Current IDM Reports**

| Report Name | Report Description |
|---|---|
| User Details Report | This report provides detailed user and role-specific information for IDM Integrated application users. |
| User Role Approver Report | This report provides information about user role requests for an application, with corresponding details of the approvers who took an action on these requests by either approving or rejecting the request. |
| Application Summary Report | This report provides a summary of the number of users registered to an application that is integrated with the IDM System. The report also includes the number of IDM account holders that do not have a role in any application. |
| Annual Role Certification Summary Report | This report displays the total count(s) of all the user roles that are certified, revoked and/or due for Annual Role Certification (ARC) by a single or multiple application. |
| Pending Annual Role Certification Report | This report displays data about all user roles that are pending or due for annual role certification. |

[52] Approved users who are granted access to My Reports will not automatically receive access to every report. A user is granted access to reports based on that user's specific role or roles.

# 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.[53]

**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 | -- | -- | -- | -- |
| 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 | X | -- | X |
| Remove Roles/Attributes | -- | O | -- | -- | -- | X |
| Promote User | -- | -- | -- | -- | -- | -- |

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

[53] 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 |
| 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: Record of Changes

**Table 8: Record of Changes**

| Version Number | Date | Author/Owner | Description of Change | Approval(s) |
|---|---|---|---|---|
| 1.09 | 04/10/2024 | Omni/Bana | Updated with new OIE screenshots | |
| 1.10 | 04/15/2024 | Omni/Bana | Text fixes | |
| 1.11 | 07/03/2024 | Omni/Bana | Updated screenshots with new Experian Phone Number on Figures 9, 11 | |
| 1.12 | 07/16/2024 | Omni/Bana | Added details on address formatting tips for “Commonwealth of Puerto Rico” in How to Request a Role Section | |
| 1.13 | 09/04/2024 | | Modified Section 11 and 16 to accommodate optional email MFA update | |