

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

# **Identity Management (IDM)**

# **User Guide**

Version 1.09 04/10/2024

Document Number: IDM User Guide Version 1.09 Contract Number: 47QTCA19D00FF:75FCMC22F0004 Last Reviewed: 04/10/2024

# **Table of Contents**

1. Introduction	
Identity Management (IDM) System Overvie User Guide Purpose	
Where to Get Help	
2. Prepare to Access the IDM System	
Verify the Web Browser is Supported	
Verify and Adjust the Screen Resolution if N Review Account Creation Instructions	
3. Overview of the IDM System	
4. How to Create a New User Account	
5. How to Sign In	9
How to Sign In (First Time Sign in - All Users	s)9
How to Sign In (All Users)	
How to Sign In with a PIV Card (CMS EUA I The IDM Self-Service Dashboard at a Gland	Jsers Only) 11
Session Expiration	
6. How to Request a Role	
How to Request a Role for a New Applicatio	
How to Request a Role for a New Applicatio 6.1.1 What to do When Users Can't Ve	n 14
6.1.1 What to do When Users Can't Ve 6.1.2 What to do When Users Can't Ve	n14 rify Their Identity with Online Proofing 17 rify Their Identity with Phone Proofing 18
6.1.1 What to do When Users Can't Ve 6.1.2 What to do When Users Can't Ve How to Request a Role in an Existing Applic	n
6.1.1 What to do When Users Can't Ve 6.1.2 What to do When Users Can't Ve	n
6.1.1 What to do When Users Can't Ve 6.1.2 What to do When Users Can't Ve How to Request a Role in an Existing Applic	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> <li>How to Cancel a Role Requests</li> <li>8. How to Remove Roles and Role Attribute</li> <li>How to Remove a Role</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> <li>How to Cancel a Role Request</li> <li>8. How to Remove Roles and Role Attribute</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> <li>How to Cancel a Role Requests</li> <li>8. How to Remove Roles and Role Attribute</li> <li>How to Remove a Role</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> <li>How to Cancel a Role Request</li> <li>8. How to Remove Roles and Role Attribute</li> <li>How to Remove a Role</li> <li>How to Remove Attributes From a Role</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li></ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li> <li>How to Cancel a Role Requests</li> <li>8. How to Remove Roles and Role Attribute</li> <li>How to Remove a Role</li> <li>How to Remove Attributes From a Role</li> <li>9. How to Initiate a Role Certification Request</li> <li>How to Change an Expired Password</li> </ul>	n
<ul> <li>6.1.1 What to do When Users Can't Ve</li> <li>6.1.2 What to do When Users Can't Ve</li> <li>How to Request a Role in an Existing Applic</li> <li>How to Add Attributes to an Existing Role</li> <li>7. How to View and Cancel Role Requests</li> <li>How to View Role Requests</li></ul>	n

User Guide Version 1.09

Identity Management (IDM)

#### Table of Contents

11. How to Manage MFA and Recovery Devices	38
How to View MFA and Recovery Devices	
How to Add an IVR or SMS MFA/Recovery Device	40
How to Activate a Pending IVR or SMS MFA/Recovery Device	41
How to Add a Google Authenticator Mobile App MFA Device	41
How to Add an Okta Verify MFA Device	
How to Add a YubiKey MFA Device	44
How to Edit MFA Device Settings	
How to Remove an MFA Device	-
12. How Manage User Account Profile Information	
How to Open and Close the My Profile Function	47
How to View User Profile Information	
How to View and Modify Personal Contact Information	48
How to View and Modify Business Contact Information	49
How to Change the User Account Password	49
How to Change the User Security Question and Answer	
13. How to Approve Role Requests	
How to Open and Close the My Approvals Function	
How to View a List of Pending Approval Requests	
13.1.1 How to View Details for a Specific Pending Approval Request	53
How to Approve or Reject a Single Request	
How to Approve or Reject Multiple Requests on a Single Page	54
How to Simultaneously Approve and Reject Multiple Requests	55
How to Export a List of Pending Approvals to an Excel Spreadsheet	
14. How to View IDM Reports	
Description of the IDM Reports Function	58
How to Access the IDM Reports	
How to Print a Report	
How to Export a Report to an Excel Spreadsheet	60
15. How to Perform Annual Role Certification	61
Annual Role Certification for Manually Approved Roles	61
15.1.1 How to Open and Close the My Annual Role Certifications Function	61
15.1.2 How to View a List of Pending Certifications	62
15.1.3 How to Perform a Global Search	
15.1.5 How to Perform an Advanced Search	
15.1.6 How to View User/Role Details and Certify/Revoke a Single User's Role	
15.1.7 How to Bulk Certify or Revoke Multiple User Roles	
15.1.8 How to use the Cart to Certify and Revoke Multiple User Roles	68
Annual Role Certification for Programmatically Approved Roles	70
15.1.9 System Notifications Sent for Users who Fail Pre-check Validation	
16. Instructions for Help Desks	72

CMS XLC

### List of Figures

Description of the Help Desk/Manage Users Functions How to Access the Help Desk Functions	72
How to Choose the Appropriate Search	
How to Perform an Application Search	
How to Perform an Enterprise Search	74
How to View a User's Profile	75
How to View a Summary of a User's Applications	76
How to Remove a Single Role	
How to Remove Multiple Roles	
How to Cancel Pending Requests How to View a User's MFA Devices	02
16.1.1 How to Remove Individual MFA Devices	03 87
16.1.2 How to Remove Multiple MFA Devices Simultaneously	
How to Update a User's Email Address	
How to Reset a User's Password (Email Reset Method)	
How to Reset a User's Password (Temporary Password Method)	
How to Unlock a User's Account	
How to Suspend a User's Account	
How to Update a User's Level of Assurance (LOA)	
How to Unsuspend a User's Account	
How to Create User Audit Reports	
How to Create Role Request Audit Reports	
How to Manage YubiKey MFA Devices for Use with IDM	
16.1.3 How to Generate the YubiKey Seed File	
16.1.4 How to Manage YubiKey MFA Devices in Okta	
16.1.5 How to Revoke a YubiKey MFA Device in Okta	01
Appendix A: Password Policy1	02
Appendix B: Summary of IDM Reports1	03
Appendix C: Requesting Configurable Help Desk Privileges1	04
Appendix D: User Audit Report Type Summary1	05
Appendix E: Acronyms1	06
Appendix F: Record of Changes1	07

# List of Figures

FIGURE 1: LOCATION OF THE HELP CENTER MENU AND LINK	2
FIGURE 2: IDM SYSTEM SIGN IN PAGE	7
FIGURE 3: MFA SETUP	10
FIGURE 4: SELF-SERVICE DASHBOARD LAYOUT	11
FIGURE 5: SESSION EXPIRING WINDOW	12

User Guide Version 1.09

### List of Figures

FIGURE 6: ROLE REQUEST WINDOW	15
FIGURE 7: ROLE REQUEST - RIDP TERMS AND CONDITIONS	15
FIGURE 8: ROLE REQUEST - ATTRIBUTE SELECTION	16
FIGURE 9: RIDP ONLINE PROOFING ERROR MESSAGE	17
FIGURE 10: EXPERIAN PHONE VERIFICATION CONFIRMATION	18
FIGURE 11: PHONE PROOFING RIDP ERROR MESSAGE	18
FIGURE 12: MANAGE MY ROLES WINDOW - USER'S EXISTING ROLES	19
FIGURE 13: ADD ROLE WINDOW	20
FIGURE 14: APPLICATION ROLES WINDOW - ROLE DETAILS VIEW	21
FIGURE 15: MY REQUESTS - ROLE REQUESTS PENDING APPROVAL	22
FIGURE 16: REQUEST DETAILS WINDOW	23
FIGURE 17: MANAGE MY ROLES WINDOW	24
FIGURE 18: EDIT ROLE DETAILS WINDOW	25
FIGURE 19: MANAGE MY ROLES WINDOW WITH MANAGE MY ANNUAL ROLE CERTIFICATIONS HYPERLINK	27
FIGURE 20: MANAGE MY ANNUAL ROLE CERTIFICATIONS WINDOW	
FIGURE 21: IDM SIGN IN WINDOW WITH SELF-SERVICE LINKS	31
FIGURE 22: IDM SELF-SERVICE CHANGE EXPIRED PASSWORD WINDOW	32
FIGURE 23: IDM SELF-SERVICE RESET PASSWORD REQUEST	
FIGURE 24: IDM SELF-SERVICE RESET PASSWORD SET NEW PASSWORD	34
FIGURE 25: IDM SELF-SERVICE FORGOT USER ID WINDOW	35
FIGURE 26: IDM SELF-SERVICE UNLOCK ACCOUNT WINDOW	36
FIGURE 27: MANAGE MFA AND RECOVERY DEVICES WINDOW	40
FIGURE 28: MY PROFILE - MY INFORMATION	48
FIGURE 29: MY PROFILE - PERSONAL CONTACT INFORMATION	48
FIGURE 30: MY PROFILE - BUSINESS CONTACT INFORMATION	49
FIGURE 31: MY PROFILE - CHANGE PASSWORD FORM	50
FIGURE 32: MY PROFILE - CHANGE SECURITY QUESTION FORM	50
FIGURE 33: MY APPROVALS WINDOW	52
FIGURE 34: MY REPORTS WINDOW	58
FIGURE 35: MY REPORTS WINDOW WITH SAMPLE REPORT (FULL SCREEN VIEW)	59
FIGURE 36: LOCATION OF THE MY REPORTS EXPORT OPTIONS BUTTON	60
FIGURE 37: MY ANNUAL ROLE CERTIFICATIONS WINDOW	62
FIGURE 38: MY ANNUAL ROLE CERTIFICATION ADVANCED SEARCH WINDOW	64
FIGURE 39: MY ANNUAL ROLE CERTIFICATION USER DETAILS	66
FIGURE 40: CERTIFICATIONS TO PROCESS WINDOW	68
FIGURE 41: CERTIFY AND REVOKE MULTIPLE USER ROLES USING THE CART FEATURE	69
FIGURE 42: APPLICATION AND ENTERPRISE SEARCH CAPABILITIES MATRIX	73
FIGURE 43: HELP DESK APPLICATION SEARCH FORM	
FIGURE 44: HELP DESK APPLICATION SEARCH RESULTS	74
FIGURE 45: HELP DESK ENTERPRISE SEARCH FORM	75

User Guide Version 1.09

### List of Tables

FIGURE 46: HELP DESK ENTERPRISE SEARCH RESULTS	75
FIGURE 47: USER DETAILS USER PROFILE TAB	76
FIGURE 48: ENTERPRISE SEARCH RESULTS - APPLICATIONS TAB	77
FIGURE 49: APPLICATION SEARCH RESULTS - APPLICATIONS TAB	77
FIGURE 50: APPLICATION SEARCH RESULTS	78
FIGURE 51: USER DETAILS APPLICATIONS TAB	79
FIGURE 52: LIST OF USER'S ROLES / ATTRIBUTES	81
FIGURE 53: USER DETAILS PENDING REQUESTS TAB	83
FIGURE 54: USER DETAILS MFA DEVICE SUMMARY	84
FIGURE 55: HELP DESK USER AUDIT SEARCH FORM	93
FIGURE 56: USER AUDIT REPORT - USER PROFILE EVENTS	93
FIGURE 57: USER AUDIT REPORT - USER AUTHENTICATION EVENTS	94
FIGURE 58: USER AUDIT REPORT - USER ACCESS EVENTS	94
FIGURE 59: HELP DESK ROLE REQUEST AUDIT SEARCH FORM	95
FIGURE 60: ROLE REQUEST AUDIT REPORT	96
FIGURE 61: YUBIKEY PERSONALIZATION TOOL STARTUP WINDOW	98
FIGURE 62: YUBIKEY PERSONALIZATION TOOL - DEVICE PRESENT	98
FIGURE 63: YUBIKEY PERSONALIZATION TOOL - SETTINGS TAB	99
FIGURE 64: YUBIKEY PERSONALIZATION TOOL - YUBICO OTP TAB	99
FIGURE 65: OKTA YUBIKEY ADMINISTRATION WINDOW	

# List of Tables

TABLE 1: SELF-SERVICE DASHBOARD LAYOUT	12
TABLE 2: MFA AND RECOVERY DEVICE SUMMARY	
TABLE 3: YUBIKEY DEVICE STATUS LIST	101
TABLE 4: SUMMARY OF CURRENT IDM REPORTS	103
TABLE 5: HELP DESK PRIVILEGES	104
TABLE 6: IDM HELP DESK USER AUDIT REPORT TYPE	105
TABLE 7: ACRONYMS	106
TABLE 8: RECORD OF CHANGES	

#### Introduction

# 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.

User Guide Version 1.09

Intr	odu	ction

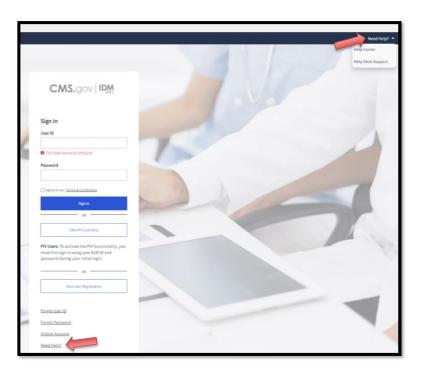


Figure 1: Location of the Help Center Menu and Link

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 <u>Tier 1</u> <u>Help Desk Support</u> website.

2

# 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.

4

#### 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.



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

Sign In User ID  Password  Agree to our Terms & Conditions  Sign In  OR  CMS PIV Card Only  PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login.  OR  New User Registration  Forgot User ID  Forgot User ID  Forgot Password		CMS.gov   IDM
Password  Agree to our Terms & Conditions  Sign In  OR  CMS PIV Card Only  PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login.  OR  New User Registration  Forgot User ID	Sigr	n In
Agree to our <u>Terms &amp; Conditions</u>	User	ID
Sign In         OR         CMS PIV Card Only         PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login.         OR         OR         New User Registration	Passv	word
OR CMS PIV Card Only PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login. OR New User Registration Forgot User ID	🗌 Ag	ree to our <u>Terms &amp; Conditions</u>
CMS PIV Card Only PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login. OR New User Registration Forgot User ID		Sign In
PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login. OR New User Registration		OR
must first sign in using your EUA ID and password during your initial login. OR New User Registration Forgot User ID		CMS PIV Card Only
New User Registration	must	first sign in using your EUA ID and
Forgot User ID		OR
		New User Registration
Forgot Password	Forg	ot User ID
	Forgo	ot Password
		I Help?

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.

User Guide Version 1.09

7

- 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.
- Select the View Terms & Conditions button. Read the IDM System terms and conditions then select the Close Terms & Conditions button.
- Select the checkbox to acknowledge agreement with the terms and conditions, then then the *Next* button. The User Contact Information window appears.
- 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. <sup>1</sup>
- 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.

<sup>1</sup> 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.

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

CMS XLC

9

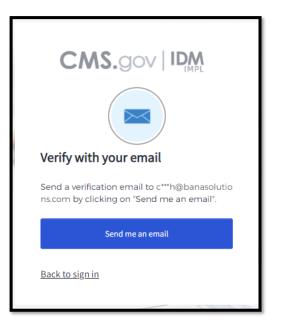


Figure 3: MFA Setup

- 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 <u>https://home.idm.cms.gov</u> The Sign In window appears as illustrated by Figure 2: IDM System Sign In .
- 2) Enter the User ID and Password.
- 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.

User Guide Version 1.09

10

# 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 <u>one</u> <u>time</u> 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

User Guide Version 1.09

11

#### 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 <b>Section 0 Where to Get Help</b> .	
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.

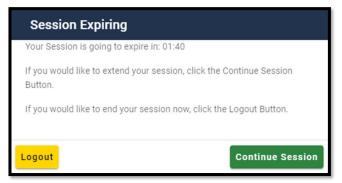


Figure 5: Session Expiring Window

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.

User Guide Version 1.09

How to Sign In

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 telephonebased 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.



#### Role Request

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

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

User Guide Version 1.09



Figure 6: Role Request Window

- 2) Select an application. The Select a Role menu appears after an application is selected. <sup>2</sup>
- 3) Select a role. The RIDP window appears after a role is selected.

Role Request				0	
Application	Role	RIDP	BCI	Review	
Remote Identity Pr	oofing				
Identity Verification - W	hat to Expect				
To complete this role reques about you.	t, it is important to note t	hat Experian, a trusted and relia	ble agent, needs to collect f	urther details	
		me, current home address, your isure a seamless and secure pr		mber, date-of-	
	For additional information or assistance, we encourage you to visit the Experian Customer Assistance website: http://www.experian.com/help				
Experian identity verification is limited to US addresses and US territories only. If you have a foreign address please call your <u>Tier</u> <u>1 Helo Desk</u> to verify your identity.					
View Terms & Condition	<u>s</u>				
I agree to the terms a	and conditions				
Cancel Back				Next	

Figure 7: Role Request - RIDP Terms and Conditions

 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.

User Guide Version 1.09

 $<sup>^2</sup>$  The Select an application menu will not display an application for which a user already has a role. To add a role to an existing application, use the *Manage My Roles* button.

5) Complete the Identity Verification form and Select the *Submit* button. The Attribute menu appears.<sup>3</sup>

Role Req	uest			8
			* Optional field	s are labeled as (Optional).
	0	0	0	4
App	lication	Role	Attributes	Review
Selected Ap T-MSIS: 1		icaid Statistical Inforr	nation System.	
mitted by s	tates on a monthly basi T-MSIS allows for busi	s. The data represent Claim	MSIS) is comprised of operational s, Eligibility, Provider, Third Party L porting on this state data stored wil	iability and Managed Care In-
View He	elpdesk Details			
Selected Ro TMSIS S	ole tate End User			
State End U	lser can view Operation	s Dashboard (OD) and Data	Quality Tool (DQT) reports for their	state.
Alaban	na, Arizona			× -
Cancel	Back			Review Request

Figure 8: Role Request - Attribute Selection

- 6) Select the required attributes.
- 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. <sup>4</sup>



- 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.

 $<sup>^{3}</sup>$  The phone number must be registered to the user who is currently navigating the RIDP workflow.

<sup>&</sup>lt;sup>4</sup> 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** 

A	We were unable to verify the information you have provided.
ubm	itted Information:
Testy	Testers
11/25	
	Big Thunder
	ntonio, TX 78245
254)	98-9396
	${\sf is}$ an error in the information you've submitted, you can modify and resubmit by clicking the retry button or you can contact Experian Support Services to complete the one-time verification process over the .
	an Support Services 985-0709
	nce Number AMPLE-12345678

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.
- If there was a mistake in the submitted personal information, select the *Retry* button. Proceed from <u>Section 6.1 Step 5</u>.
- 3) 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.

To cont	inue, please select the following:
۲	Yes, I have called Experian to proof my identity.
	Save home address to my profile
0	No, I have not called Experian to proof my identity. I need to restart the identity proofing process.
f you h resolve.	ave already contacted the Experian Support Services and failed identity proofing, call your Tier 1 Help Desk to further

#### 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**.

A	IDM has no record of your successful identity proofing. Please contact Experian Support Services to resolve issue.	×
	e contact Experian Support Services to complete the one-time verification	
proce	ss over the phone.	
	an Support Services	
1-833	-985-0709	
Refer	ence Number	
	AMPLE-12345678	

#### 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.

User Guide Version 1.09

- If Phone Proofing was successful, select **Back**. Select the "Yes, I have called Experian to proof my identity" radio button. Select **Continue**.
- 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 <u>Tier</u> <u>1 Help Desk Support</u> 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.

Manage My Roles						
Application Name 🔨	Role Name	Actions				
T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	⑦ 왇 ⁺ × × 2				
Did you know roles need to be certified by your Approver once a year? You have the option to notify your Approver of your desire to have your role certified by clicking here.						

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



 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. <sup>5</sup>

<sup>5</sup> 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.

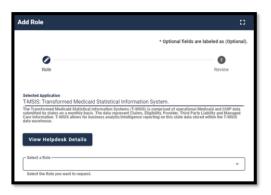


Figure 13: Add Role Window

- 4) Select a Role. The Attribute menu appears.
- 5) Select the required attributes.
- 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. <sup>6</sup>



 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.



 $<sup>^{6}</sup>$  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.

Application Roles		8
T-MSIS: Transformed Medicaid Statistical	Information System.	
TMSIS State End User	Role: Assigned Date: State:	TMSIS State End User 05/20/2022 Alaska, Alabama
Go to My Roles	I	Remove Role Modify 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. <sup>7</sup>
- 7) Select the Go to My Roles button. The Manage My Roles window appears and the My



Requests indicator **control** 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.  $^{8}$   $\overset{0}{9}$ 

Request ID	Application	Role	Approval Attribute	Attribute Value(s)	Submit Date	Expiration Date	Action	
1824331	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Connecticut	05/20/2022 04:30 PM	05/21/2022 04:30 PM	21	*8
1824332	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Dist of Columbia	05/20/2022 04:30 PM	05/21/2022 04:30 PM	21	*8
824333	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Delaware	05/20/2022 04:30 PM	05/21/2022 04:30 PM	21	*8
1824334	T-MSIS: Transformed Medicald Statistical Information System.	TMSIS State End User	State	Florida	05/20/2022 04:30 PM	05/21/2022 04:30 PM	21	*8
1824335	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Georgia	05/20/2022 04:30 PM	05/21/2022 04:30 PM	21	*8

Figure 15: My Requests - Role Requests Pending Approval

 $<sup>^{\</sup>rm 8}$  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.

 $<sup>^{9}</sup>$  (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.

Application:	T-MSIS: Transformed Medicaid Statistical Information System.
Role:	TMSIS State End User
Request ID:	1824338
Submit Date:	05/20/2022
Expiration Date:	05/21/2022
Reason for Request:	Test User
State:	Idaho

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

2) Select the Cancel Request button



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.



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.

 $<sup>^{10}</sup>$  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.

Manage My Roles			8
Application Name	Role Name	Actions	
T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	<ol> <li>2/ +음</li> </ol>	×۲
MIDAS SAS Web	MIDAS SAS User	⑦ ೭/ +8	×۵
Special HIH	Basic user	<u> ?</u> 원 +원	×۵
Did you know roles need to be certified by your Approver on Approver of your desire to have your role certified by clickin	,	option to notify y	our

Figure 17: Manage My Roles Window



2) Select the Remove Role button.

The Remove Role decision window appears.

Identity Management (IDM)

- 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. <sup>11</sup>
- 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.



- 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.
- 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.  $^{12}$

Edit Role Details	0
* Optional fields are labeled as (Optional).	
Application: T-MSIS: Transformed Medicaid Statistical Information System. Role: TMSIS State End User Date Assigned: 03/20/2022	
Arizona, Alabama × *	
Reason for Request Test user removes the California attribute.	
Enter a reason for request using 1 to 600 alpha mameric and special characters, except less than (-), greater than (-) o parentheres ().	r
Cancel Sub	mit

Figure 18: Edit Role Details Window

4) Remove the desired role attributes.

 $<sup>^{11}</sup>$  An email is sent to the user's email address of record which indicates that the request was accepted.

<sup>&</sup>lt;sup>12</sup> 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.

- 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. <sup>13</sup>
- Select the Go to My Roles button. The Manage My Roles window appears and displays the user's current roles.

 $^{13}\,\mbox{An email}$  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.



 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.

oplication Name	Role Name	Actions
IDAS SAS Web	MIDAS SAS Helpdesk	<ol> <li>관 · 음 · 음</li> </ol>
RIS Plan Portal	EPOC User	🧿 🌮 +8 😕
edicaid Data Collection Tool Quality Measures Reporting (MDCT QMR)	MDCT QMR Business Owner Rep	🧿 🌮 +8 ×8
s&R/STAR here.	PS&R/STAR Helpdesk	<ol> <li>2 + 음 × 음</li> </ol>
s&R/STAR here.	· · · · · · · · · · · · · · · · · · ·	

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

User Guide Version 1.09

How to Initiate a Role Certification Request



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.

Manage My Annual	Role Certification						0
Search			٩			G	9 R
If you no longer requi	ire a role listed below please remov	e that role via Manage My Roles.			4 of the 4 role	e certifications have be	en loaded.
Application	Role	Attribute	Certification Status 🛧	Next Review Date	Last Review Date	Actions	
PS&R/STAR	PS&R/STAR Helpdesk	N/A	Certification Due	08/09/2022		$\odot$	
MIDAS SAS Web	MIDAS SAS Helpdesk	N/A	Certification Due	08/09/2022		۲	
PRIS Plan Portal	EPOC User	Plan Contract Number: H1111	Certified	05/23/2023		۲	
PRIS Plan Portal	EPOC User	Plan Contract Number: H2222	Certified	05/23/2023		÷	
			< 1 >			Results Per Page	× •

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).

User Guide Version 1.09

28

Identity Management (IDM)

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



The Certification(s) to Request window appears.

- $\otimes$
- 8) Select the *Remove from Cart* button. **I** 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.

CMS XLC

7) Select the View Cart button.

# 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.

CMS.gov   IDM
Sign In
User ID
Password
Agree to our <u>Terms &amp; Conditions</u>
Sign In
OR
CMS PIV Card Only
PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login.
OR
New User Registration
Forgot User ID Forgot Password
Need Help?

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.

User Guide Version 1.09

31

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 <u>Tier 1 Help Desk Support</u> 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.

our password has expired
ssword requirements:
At least 15 characters
A lowercase letter
An uppercase letter
Anumber
No parts of your username
Does not include your first name
Does not include your last name
Your password cannot be any of your last 6
passwords
At least 1 day(s) must have elapsed since you last changed your password
ew password
-enter password

Figure 22: IDM Self-Service Change Expired Password Window

- 1) Enter the New Password and the Repeat Password.
- 2) Select the *Change Password* button. <sup>14</sup>

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 <u>Password</u> 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.

CMS.g	ov   IDM Self Service
R	eset Password
User ID	
The	User ID field is required.
	Call can only be used if a number has been configured.
	Reset via SMS
Re	eset via Voice Call
	Reset via Email
<u>Back to sign in</u>	

Figure 23: IDM Self-Service Reset Password Request

- 2) Enter the User ID.
- 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.

<sup>&</sup>lt;sup>14.</sup>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. <sup>15</sup>
- 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.

CMS.gov   IDM Self Service	
New Password	
	Ø
The New Password field is required. Confirm Password	
	Ø
Reset Password	
Back to Sign In	

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.
- 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.

<sup>&</sup>lt;sup>15</sup> 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 <u>User ID</u> 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.

Forgo	ot User ID
E-mail Address	
The E-mail Add First Name	ress field is required.
.ast Name	
Date Of Birth	
Date Of Birth	
	US or Foreign Address?
MM/DD/YYYY Is your Address a l	US or Foreign Address?
MM/DD/YYYY Is your Address a l	, i i i i i i i i i i i i i i i i i i i
MM/DD/YYYY Is your Address a l O US Address	, i i i i i i i i i i i i i i i i i i i
MM/DD/YYYY Is your Address a I US Address Cip Code 00000	, i i i i i i i i i i i i i i i i i i i

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.

- 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. <sup>16</sup>
- 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 <u>Unlock</u> 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.

CN	IS.gov   IDM Self Service
	Unlock Account
User ID	
	The User ID field is required.
	/oice Call can only be used if a hone number has been configured.
	Send SMS
	Voice Call
	Send Email
Back to si	gn_in

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.

<sup>&</sup>lt;sup>16</sup> 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.  $^{\rm 17}$ 

Table 2: MFA and Recovery Device Summary

MFA Device	Device Type	Actions	Modifiable Setting	Edit Settings
Email	MFA & Recovery	Modify	Email Address	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.

User Guide Version 1.09

<sup>&</sup>lt;sup>17</sup> 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.

Manage MFA and Recovery Devices

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

Table 2: MFA and Recovery Device Summary.

User Guide Version 1.09

My Profile					G ::
My Information Personal Contact Information Business Contact Information Change Password	Manage MFA and R The devices managed on this pa all users. The same devices are required to login with MFA for th required for your role or applicat	ge are used for self-se also used for Multi-Fa eir role or application.	ervice password res ctor Authentication	(MFA) logins but only apply to	those users
Change Security Question Manage MFA and Recovery Devices	Type E-mail Address	Value johnhs@c- hit.com	Status Active	Device Type Recovery/MFA for E- mail	Actions
	Interactive Voice Response (IVR)	+14107870981	Pending Activation	Recovery/MFA for voice	2/ ×8
	Text Message (SMS)	+14107870981	Active	Recovery/MFA for SMS	×Q
	Add another device Adding a MFA Code to your login at layer of protection to your User ID as unable to register your MFA device v	so known as Multi-Factor A Id Password. Please note vithin two attempts please	Authentication (MFA), c that you are only allowe log out, then log back i	an make your login more secure by d two atternpts to register your MF in to try again.	providing an extra A device. If you are

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.

- 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.
- 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.
- 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.
- 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.

User Guide Version 1.09

40

#### CMS XLC

### 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.

- 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.
- 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.

- 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.
- 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.
- 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.

41

- Download and install the Google Authenticator mobile app onto the mobile device. Obtain the app from the appropriate app store.
- 7) Select the *Register Device* button on the IDM Google Authenticator setup window. The window displays a QR code.
- Start the Google Authenticator app on the mobile device and select the *Get Started* button. The Account Setup screen appears.
- 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.<sup>20</sup>
- 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.
- 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.
- Use the Add another device menu to select the Okta Verify option. The Okta registration window opens.
- Select the Next button and follow the on-screen prompts for installing an Okta Verify MFA device.

<sup>&</sup>lt;sup>19</sup> 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.



<sup>20</sup> 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.

User Guide Version 1.09

42

- Download and install the Okta Verify app onto the mobile device. Obtain the app from the appropriate app store. <sup>21</sup>
- 7) Select the *Register Device* button on the IDM Okta Verify setup window. The window displays a QR code.
- Start the Okta Verify app on the mobile device. The Welcome to Okta Verify screen appears.
- 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
- A message is displayed which indicates the MFA device was successfully added. Select the OK button.

 $<sup>^{21}</sup>$  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.



<sup>22</sup> 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.

User Guide Version 1.09

# 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.

- 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.
- 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.
- Use the Add another device menu to select the YubiKey option. The YubiKey registration window opens.
- 5) Select the YubiKey Passcode field.
- 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.
- 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.

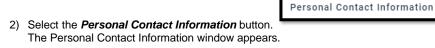
**Note:** The Email MFA device uses the same email address that stored in the user's IDM profile.

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

User Guide Version 1.09

44

 Select the *My Profile* button as described in Section 0 How to Open and Close the My Profile Function. The My 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.  $^{\rm 23}$ 

**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.

- 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.
- 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.

User Guide Version 1.09

 $<sup>^{23}</sup>$  Users who are required to use email as the default MFA device will not have the option to remove the Email MFA device.

How to Manage MFA and Recovery Devices

CM	S 2	XL	С

×°

- 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

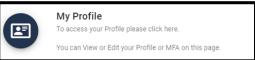
Users view and edit their user account profile information using the IDM Self-Service My Profile Function. This function enables users to view and/or modify various attributes of their user profile to include:

- 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 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.

IDM Self Service

# 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.

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

47

located at the top left

Profile		c	8
Ay Information Personal Contact Information	My Information		
Business Contact Information	User ID:	johnjowner	
change Password	Title:		
Change Security Question	First Name:	John	
Nanage MFA and Recovery Devices	Middle Name:	Jimmy	
	Last Name:	Sandwich	
	Suffix:		
	Date Of Birth:	10/13/1979	
	Last 4 of SSN:	8909	

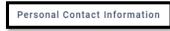


## How to View and Modify Personal Contact Information

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

#### **View Personal Contact Information**

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



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

y Profile			c ::
My Information Personal Contact Information	Personal Contact In	formation	/
Business Contact Information	E-mail Address:	johnhs@c-hit.com	
Change Password	Home Address Line 1:	328 Dart St	
Change Security Question	Home Address Line 2:		
Manage MFA and Recovery Devices	City:	Middletown	
	State:	DE	
	Zip Code:	39825	
	Zip Code Extension:		
	Phone Number:	5444325832	

Figure 29: My Profile - Personal Contact Information

### Modify Personal Contact Information

- With the Personal Contact Information window open, select the *Edit* button. 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.

User Guide Version 1.09

The

## 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**

 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.

My Profile			c ::
My information Personal Contact Information	Business Contact Info	ormation	1
Business Contact Information	Professional Credentials:		
Change Password	Company Name:	Affluent Health Care	
Change Security Question	Address Line 1:	1313 Mockingbird Rd	
Manage MFA and Recovery Devices	Address Line 2:		
	City:	Big Bend	
	State:	IA	
	Zip Code:	43940	
	Zip Code Extension:		
	Company Phone Number:	432-657-4300	
	Company Phone Extension:		
	Office Phone Number:	432-657-4302	
	Office Phone Extension:		

Figure 30: My Profile - Business Contact Information

#### Edit the User's Business Contact Information

- With the Business Contact Information window open, select the *Edit* button.
   Business Contact Information becomes modifiable.
- 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.

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

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

User Guide Version 1.09

The

y Profile		
My information Personal Contact Information	Change Password	
Business Contact Information Change Password	Current Passanut	C
Change Security Question Manage MFA and Recovery Devices	Men Passaul	C
	Contine Password	G
		Change Password

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.

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



 Select the Change Security Question button. The Change Security Question window appears.

My Profile	8
My information Personal Contect Information Business Catalox Information Change Rescutty Question Change Rescutty Question Manage MFA and Recovery Devices	Change Security Question

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. <sup>24</sup>
- 5) Enter the Current Password.
- 6) Select the Change Security Question button.

User Guide Version 1.09

Identity Management (IDM)

 $<sup>^{24}</sup>$  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. <sup>25</sup>

 $^{25}$  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.

User Guide Version 1.09

#### 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.

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

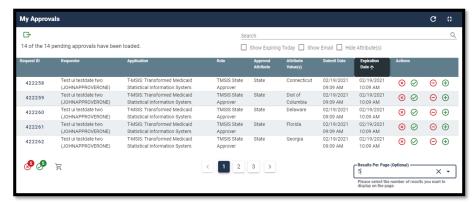


Figure 33: My Approvals Window

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. <sup>26</sup>

<sup>26</sup> 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.

Request ID 131316

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

- 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.
- Select the Go to My Approvals button to close the Pending Approval Details window. The Approver returns to the My Approvals window.<sup>27</sup>

## 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.

- 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.

	$\oslash$	
1	_	

- 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.
- Select the Submit button. The IDM System displays a message which indicates the operation completed successfully. The My Approvals indicator decrements by one.
- Select the Go to My Approvals button. The Approver returns to the My Approvals window.

<sup>&</sup>lt;sup>27</sup> The Pending Approval Details window also provides the capability to approve or reject a single request that is pending approval. Refer **Section 0 How to Approve or Reject a Single** Request.

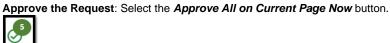
### How to Approve or Reject Multiple Requests on a Single Page

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.

 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 **b** 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 or Reject list (Optional). 28

. 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).



to remove a specific request from the

- 6) Enter a brief justification. The same justification will be applied to each request.
- Select the Submit button. All records that appear on the Pending Approvals to Process list will be processed as Approvals or Rejections.

<sup>&</sup>lt;sup>28</sup> 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.

- 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.

 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 **b** to change the number of requests that are displayed on each page in the My Approvals window (Optional).
- Select the appropriate button to approve or reject <u>each individual request</u> 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.

Approval/Rejection action (Optional). 29

5) Select the *Remove Request* button

to remove a specific request from the bulk

The Pending Approvals to Process window appears.

Identity Management (IDM)

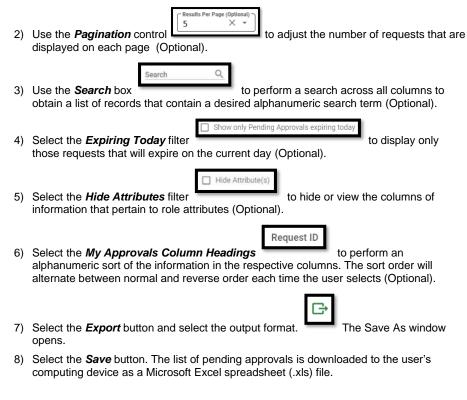
<sup>&</sup>lt;sup>29</sup> The specific record will be removed from the Pending Approvals to Process list and will remain in pending status. The Approver will receive periodic email reminders about the pending requests until they are acted on, or they expire.

- 6) Enter a justification for the Rejections <u>and</u> a justification for the Approvals. The same rejection or approval justification will be applied to each rejected or approved request respectively.
- Select the Submit button. All records that appear on the Pending Approvals to Process list will be processed as Approvals or Rejections.
- 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.
- 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.

 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.



User Guide Version 1.09

56

CMS XLC

How to Approve Role Requests

User Guide Version 1.09

# 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.



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

My Reports	
C Solect a Report	•

Figure 34: My Reports Window

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

CMS.gov   IDM Se	If Service I		2 20 🖻							දුරී ලී Ricky Helper 👻
My Reports			MCU Test0					× •		4
			Select a Report from the options			1.				Contraction of the
0 0 3	-	Report	Selection Butto	ons	R	eport Filters				Print
ICU Counts Requests	Approved Reg	uests Rejected Role	Removal Details		-					_
ntrols Role Removal D	ata Dana Gun Jan O	20 Pala Paran	ral Date To Sat Sep 30 202 Rec	uest ID All Role I	Name All Requested B	y All User First Name All	User Last Na			
TITOIS KOLE KEMOVALD				Uest ID All Role I	Name All Requested b	y All User First Name All	User Last Na	<b>100</b> All		
otal Count 1,334		<b>Total Reco</b>	rd Count							
	-				Column	1 Headers				
					Colum	1 Headers				
ker ID	First Name	Last Name	Email	Phone Number	Last Login Timestamp	Role Revoked	Request ID	Role Revoked Date	Rennest Status	
M AUTO RR NET V1 1	IDM Verticals	NetVOne One	cms.chit.idmtest/Bgmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADMINISTRATOR	586304	Feb 24, 2021	Role Revoked	· · · · · · · · · · · · · · · · · · ·
M AUTO RR NET V1 1	IDM Verticals	NetVOne One	cms.chit.idmtest@omail.com	2024305826	03/20/2021 06:08 AM	MCU ADMINISTRATOR	603308	Mar 3, 2021	Role Revoked	Export
M AUTO RR NET VI 1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU ADMINISTRATOR	645085	Mar 20, 2021	Role Revoked	Options
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADVANCED_RESOLUTION	586364	Feb 24, 2021	Role Revoked	options
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADVANCED_RESOLUTION	603368	Mar 3, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 05:08 AM	MCU_ADVANCED_RESOLUTION	645129	Mar 20, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_BUSINESS_OWNER_REP	586313	Feb 24, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_BUSINESS_OWNER_REP	645089	Mar 20, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_HELPDESK	586323	Feb 24, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_HELPDESK	603331	Mar 3, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_HELPDESK	645093	Mar 20, 2021	Role Revoked	- Report Bod
DM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_1	586335	Feb 24, 2021	Role Revoked	Report Bou
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_1	603342	Mar 3, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_1	645097	Mar 20, 2021	Role Revoked	
M AUTO RR NET VI 1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_2	586345	Feb 24, 2021	Role Revoked	
	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_2	603350	Mar 3, 2021	Role Revoked	
	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_2	645101	Mar 20, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1		NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_USER_APPROVER	\$86355	Feb 24, 2021	Role Revoked	
M_AUTO_RR_NET_V1_1	IDM Verticals				03/20/2021 06:08 AM	MCU_USER_APPROVER	603356	Mar 3, 2021	Role Revoked	
DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1	IDM Verticals IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826						
DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1		NetVOne One NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_USER_APPROVER	645105	Mar 20, 2021	Role Revoked	Page Size
DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1 DM_AUTO_RR_NET_V1_1	IDM Verticals					MCU_USER_APPROVER MCU_ADMINISTRATOR	645105 564383	Mar 20, 2021 Feb 16, 2021	Role Revoked	Page Size

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

	Role Removal Details
reports are available. For example:	

4) Filter report columns: Select a Report Filter button to filter the report to display specific

Role Name

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

ge size 500

displayed on the screen (Optional). For example:

User Guide Version 1.09

# 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**.

B
Ψ

- 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**.
- If the Export Options button is not visible, select on any row of the *Report Body* (Optional).

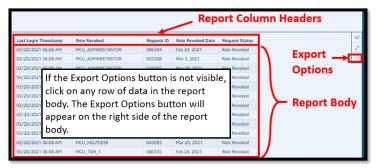


Figure 36: Location of the My Reports Export Options Button



- 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.

User Guide Version 1.09

60

# 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:**



 Select the My Annual Role Certifications button 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.

User Guide Version 1.09

61

• 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.

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

My Annual Role Certi	fications									
Search				٩	Advanced Search			G	ی کی	E
Due Date Filter (Optional) -	X 👻 🗹 Show Em	ail Address 🔽 Show I,	Iser Requested				2947 of th	ne 2947 role certification	ns have been loa	aded.
User	Email Address	Application	Role	Attribute	User Requested 🕹	User Requested Date	Certification Due Date	Last Certified On	Actions	
TestsubThree DoeThree (ITESTDOES3)	johnhs@c-hit.com	MIDAS SAS Web	MIDAS SAS Helpdes	N/A	Yes	05/25/2022	08/09/2022		⊖ ⊕	
qw qwertyuiplikijhgfdsazxc v (TPTSTUSER73)	pkittu12@mailinator.c om	CCIC Netsparker	CCIC Netsparker Analyst	N/A	*.		06/25/2022		⊖ ⊕	
mfa delete a (DELETEMFALOA3)	NavaneethaS@c- hit.com	PRIS Plan Portal	EPOC User	Plan Contract Number: H1111	2		07/09/2022		⊖ ⊕	
mfa delete a (DELETEMFALOA3)	NavaneethaS@c- hit.com	PRIS Plan Portal	EPOC User	Plan Numl H222	Displa	ays the	number	of role		٦
mfa delete a (DELETEMFALOA3)	NavaneethaS@c- hit.com	PRIS Plan Portal	EPOC User	Numi S058	rtificatio				aded.	
mfa delete a (DELETEMFALOA3)	NavaneethaS@c- hit.com	PRIS Plan Portal	EPOC User	Plan Contract Number: \$0655			0770972022		⊖ ⊕	
Sherley Ayala (SYTSTUSER10)	SiddharthaY@c- hit.com	PRIS Plan Portal	Admin User	N/A	÷		08/09/2022		⊖ ⊕	
Cherry Test (CHERRY_TEST1)	sadhanay@c-hit.com	T-MSIS: Transformed Medicaid Statistical Information System.		N/A	-		08/09/2022		⊖ ⊕	
		¢	1 2 5	8 59 >			Results P 50			× •
							Please se	lect the number of results you		Top

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.

User Guide Version 1.09

CMS XLC	C How to Perform Annual Role Certification
4)	Use the <b>Due Date</b> filter Optional X T to display only those users whose certifications expire during the desired timeframe (Optional).
5)	Select the <b>Show Email Address</b> filter address column (Optional).
6)	Select the <b>Show User Requested</b> filter to hide or view the User Requested and User Requested Date information columns (Optional).
7)	Select any <i>Column Heading</i> to sort the list based on the contents of that column (Optional).
15.1.3	B How to Perform a Global Search
Global	I Search enables Approvers to perform a keyword search across all information (including tributes if applicable) to narrow the results of the records in their pending role certification
	: If an Approver has more than 1000 user roles pending role certification, only the first pending role records can be searched using Global Search.
	<b>e:</b> The <b>Show Email Address</b> box must be selected if you want to perform a Global ch that is based on a user's email address.
	perform a global search using the following procedure.
1)	Select the <i>My Annual Role Certifications</i> button as described in <b>Section 0 Annual</b> <b>Role Certification.</b> The My Annual Role Certifications window appears as illustrated by <b>Figure 37: My Annual Role Certifications Window</b> .

2) Enter a keyword into the Search field.

Search	Q
--------	---

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.

 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.

		Advanced Search	
2)	Select the <i>Advanced Search</i> button. window appears.		The Advanced Search

Advanced Search	
User ID (Optional)	
First Name (Optional)	Last Name (Optional)
Due Date Filter (Optional)	
Certification Date From (Optional)	Certification Date To (Optional)
User Requested (Optional)	
_ Application	
Cancel Clear Fields	Certification Search

#### 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).

User Guide Version 1.09

64

- 7) Select the *Certification Search* button.
- 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.

 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. appears.

The User Details window

Personal Information	
User ID:	ANDY.SMITH0105
First Name:	hh
Last Name:	qwertyuioplkjhgfdsazxcvbn
E-mail Address:	brijeshkumarp@c-hit.com
Request Details Certification Due Date:	06/21/2022
Last Certified On:	
User Requested:	Yes
User Requested Date:	05/13/2022
Application:	MA/MA-PD/PDP/CC
Role:	EPOC
Plan Contract Number:	\$8841
Business Contact Informati Company Name:	kidi
Address Line 1:	lididilid
Address Line 2:	
City:	lklill
State:	IA
Zip Code:	43434
Zip Code Extension:	4343
Company Phone Number:	434-344-4444
Company Phone Number Extension:	
Office Phone Number:	444-444-4444
Office Phone Number Extension:	
<ul> <li>I acknowledge that I am responsible role.</li> </ul>	e for certifying or revoking my users' continued use of the assigned
- Reason for Decision (Optional)	

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.

User Guide Version 1.09

66

### 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.

 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.

certification.



flag all roles displayed on the page for

Or



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

a. Select the Certify all button

to flag all roles displayed on the page

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

Jser	Application	Role	Attribute	Certification Due Date	Last Certified On	Action	Actions
FestsubThree DoeThree ITESTDOES3)	MIDAS SAS Web	MIDAS SAS Helpdesk	N/A	08/09/2022		CERTIFY	$\otimes$
ąw ąwertyuipikjhgfdsazxcv TPTSTUSER73)	CCIC Netsparker	CCIC Netsparker Analyst	N/A	06/25/2022		CERTIFY	$\otimes$
nfa delete a DELETEMFALOA3)	PRIS Plan Portal	EPOC User	Plan Contract Number: H1111	07/09/2022		CERTIFY	$\otimes$
nfa delete a (DELETEMFALOA3)	PRIS Plan Portal	EPOC User	Plan Contract Number: H2222	07/09/2022		CERTIFY	$\otimes$
Sushma Boyapati (BXL3)	MIDAS SAS Web	MIDAS SAS Web Admin	N/A	08/05/2022		CERTIFY	$\otimes$
Patrick Faulkner SYTSTUSER09)	PRIS Plan Portal	PRIS Plan Portal Help Desk User	N/A	08/09/2022		CERTIFY	$\otimes$
Sherley Ayala SYTSTUSER10)	PRIS Plan Portal	Admin User	N/A	08/09/2022		CERTIFY	$\otimes$
Cherry Test CHERRY_TEST1)	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS CMS Power User	N/A	08/09/2022		CERTIFY	$\otimes$
		< 1 >					
I acknowledge that I a	m responsible for certifying or revoking my us	sers' continued use of the assigned rol	e.				
ertify - Reason for Decision (Op	ational)						
							0 / 600

Figure 40: Certifications to Process Window

7) Select the *Remove from Cart* button

to reverse the certify or revoke action for a

8) Select the *Acknowledge* box.

single role (Optional).

- 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.

 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.

User Guide Version 1.09

68

How to Perform Annu	al Role Certification
---------------------	-----------------------

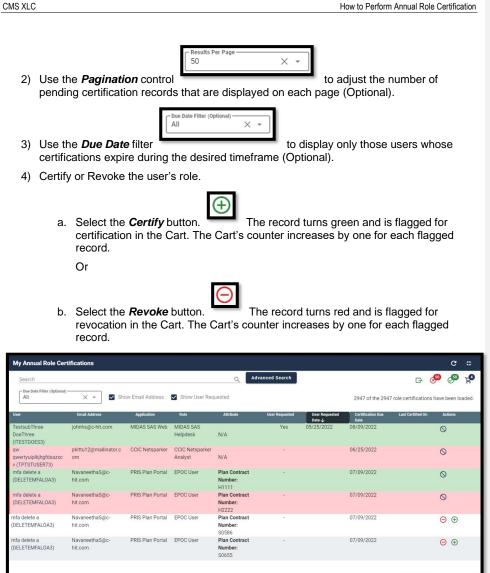


Figure 41: Certify and Revoke Multiple User Roles using the Cart Feature

< 1 2 ... 58 59 >

- 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).

User Guide Version 1.09

- Resu 50



- 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).
- 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<sup>st</sup> 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<sup>st</sup> 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<sup>st</sup> certification due date for programmatically approved roles.

The initial email is sent 90 days before the June 1<sup>st</sup> certification due date. Subsequent reminder emails are sent at 60 days, 30 days, 7 days, and 1 day before the June 1<sup>st</sup> 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<sup>st</sup> 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

User Guide Version 1.09

Identity Management (IDM)

CMS XLC

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.

User Guide Version 1.09

## 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 LOA
- 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		-			-	100 B
Update User Email Address	Appl & Ent Srch	Appl & Ent Srch	-	Appl & Ent Srch	Appl & Ent Srch			-	100 A
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			
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			
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			
View List of MFA Devices	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch			
Legend: Appl = Application Sea	rch 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.

Search	
Application Search	* Optional fields are labeled as (Optional).
Application Search Enterprise Search	h
Please select an Application and at least one oti	her search critiera to perform your search.
User ID (Optional)	E-mail Address (Optional)
- First Name (Optional)	Last Name (Optional)
Application T-MSIS: Transformed Medicaid Statistica	I Information System. X 🔹
C Role (Optional)	~
Clear Fields	Application Search

Figure 43: Help Desk Application Search Form

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

Search	Results							
Search	Results for: M	arketplace Change	Utility (MCU)				Back to Sea	rch
Total F	Results: 1			Filter				Q
, u	User ID	Name	E-mail Address	State	Status	LOA	Actions	
~	JOHNENDUSER2	James App Userman	johnhs@c-hit.com	West Virginia	Get User Status	3	Click Get User Status to see actions	

#### Figure 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 <u>and</u> Last Name, <u>or</u> a User ID, <u>or</u> 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.

- 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.

Enterprise Search

The Enterprise Search Form appears.

User Guide Version 1.09

74

Identity Management (IDM)

Search	
Enterprise Search	* Optional fields are labeled as (Optional).
Application Search Enterprise Search	
Enterprise Search requires at least First Name and La search.	st Name or User ID or Email Address in order to perform a
User ID (Optional)	E-mail Address (Optional)
First Name (Optional)	Last Name (Optional)
Date of Birth (Optional) MM/DD/YYYY	Last 4 SSN (Optional)
State (Optional)	
Clear Fields	Enterprise Search

Figure 45: Help Desk Enterprise Search Form

- 3) Enter any combination of User ID or Email Address or First Name and 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).
- 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.
- Select the *Enterprise Search* button. The screen refreshes and the search results appear.

Search	Resu													
Search R	esults												Back to Sea	arch
Total Re					F	ilter								Q
User ID		Name	E-mail Address	Status	LOA	Last Login	State	Source	Action	6				
JOHNENDU:	SER2	James App Userman	johnhs@c- hit.com	ACTIVE	3		West Virginia	cmsidm2	55	Ð	÷	2	0 <del></del>	

Figure 46: Help Desk Enterprise Search Results

 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.

 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 screen refreshes and the search results appear.

User Guide Version 1.09

75

Instructions for Help Desks

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

	2 6 AL #
James	
Userman	
ACTIVE	
johnhs@c-hit.com	
02/10/1975	
3	
L337722385	
8079	
	Userman ACTIVE Johnha@c-hit.com 02/10/1975 3 L337722385

#### Figure 47: User Details User Profile Tab



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.

 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 screen refreshes and the search results appear.

#### JOHNAPPROVERONE

- 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.

User Guide Version 1.09

76

Identity Management (IDM)

Search Results Details		
Jser Details for : JOHNAPPROVERONE		Back to Results
User Profile Applications MFA		ST 🗗 🖯 🚑 👎
Application	Role	Assigned Date
BCRS Web	BCRS CMS/CAA	08/03/2020
T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	11/30/2020
Marketplace Change Utility (MCU)	MCU Business Owner Representative	12/18/2020
IDM Reports	IDM Reports - Application Business Owner Representative	02/24/2021

Figure 48: Enterprise Search Results - Applications Tab

Search Results Details	
User Details for : JOHNAPPROVERONE	Back to Results
User Profile Applications MFA	⊡ ÷ ೭ ♀
Applications	
BCRS Web	~
T-MSIS: Transformed Medicaid Statistical Information System.	~
Marketplace Change Utility (MCU)	~

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. <sup>30</sup>
- 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.

User Guide Version 1.09

 $<sup>^{30}</sup>$  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.

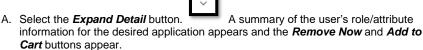
**Note:** The IDM System will display a warning message if the role removal or attribute removal operation will remove the last approver of an organization that still has users associated with that role or attribute. Such users could be left in an "orphaned" state without an approver of record for future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



earch Results for: In	ternet Server (ISV)					B	ack to Searc
otal Results: 1			Filter				
User ID	Name	E-mail Address	State	Status	LOA	Actions	
CAROLENDUSER3	Carol Userwoman	johnhs@c-hit.com	Tennessee	Get User Status	3	Click Get User Status to se	e actions
Role	Attribu	te		Attribute Value(s)		Actions	
Internet Server User	Busine	ess Application(s)		TCP, UDP, IPV, HDS		回済	
回答					Rows per page:	10 🔻 1-1 of 1	< >

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.

Instructions for Help Desks

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.

Details for : CAROLEND	USER3				Back to	Res
r Profile Applications	Pending Requests	MFA			<b>a</b> 🙃 🛱	2
oplications						
nnexion						
NTRAN						
Internet Server (ISV)						^
Role	Assigned Date		Attribute	Attribute Value(s)	Actions	
Internet Server User	03/18/2021		Business Application(s)	TCP, UDP, IPV, HDS	回茶	
回岸				Rows per page: 10	) <del>v</del> 1-1 of 1 <	>

Figure 51: User Details Applications Tab



for the role that requires removal. The

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

3) Select the Remove Now button

Remove Role/Attribute window appears.

 The Help Desk UI displays Request ID information and a message that informs the Help Desk User that the request was successfully submitted. <sup>31</sup>

 $<sup>^{31}</sup>$  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.

User Guide Version 1.09

80

Total Results: 1			Filter					
	User ID	Name	E-mail Address	State	Status	LOA	Actions	
^	CAROLENDUSER3	Carol Userwoman	johnhs@c-hit.com	Tennessee	Get User Status	3	Click Get User Status to	see actions
Ro	le internet interne	Attri	sute(s)			_	Actions	_
MACPro State User		СМ	S Region:	CMS Region 2	New York NY		ii 🛌	
		Sta	es and Territories:	New York				
M	ACPro State User	CM	S Region:	CMS Region 2	New York NY		回岸	
		Sta	es and Territories:	New Jersey				
MACPro State User		CM	S Region:	CMS Region 2	New York NY		□ 苫	
		Sta	es and Territories:	Puerto Rico				

Figure 52: List of User's Roles / Attributes



3) Select the Add to Cart button

(Optional).

4) Select the Remove from Cart button

for the individual role that requires removal. The *Remove From Cart* button appears. <sup>32</sup>



for any role that should not be removed



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

<sup>32</sup> 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).

User Guide Version 1.09

Identity Management (IDM)

for any role that

 Select the *Remove All Now* button. appears. <sup>33</sup>

The Remove Role/Attribute window



- Review the list and select the *Remove from Cart* button 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. <sup>34</sup>

## 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.



- Select the User ID for the desired user. The screen refreshes, the User Details window appears and displays User Profile information.
- Select the *Pending Requests* tab. requests appears.

Pending Requests

A list of the user's pending

<sup>33</sup> 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.

User Guide Version 1.09

User Profile	Applications Pending Requests	MFA				:: D	ĉ 2, °
						🗆 ні	de Attribute
Request Key	Application	Role	Approval Attribute	Attribute Value(s)	Submitted Date	Due Date	Actions
456771	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Alaska	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	Ô
456772	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Alabama	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	Ō
456773	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Arkansas	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	Ō
456774	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Arizona	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	Ō
456775	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	California	3/16/2021, 10:17:12 AM	3/16/2021, 11:17:12 AM	Ō

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. <sup>35</sup>

### 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.

 $<sup>^{35}</sup>$  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.

- 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.

MFA The MFA device summary appears.

Search	Results	Details							
User De	User Details for : DIZZY0						Bac	k to Re	sults
User	Profile App	olications Pending Requests	MFA		65	æ	ô	2	0+
	Factor	Device	Provider	Status	Create Date	Actio	ns		
	Email	devon@banasolutions.com	OKTA	ACTIVE		ß			_
	SMS	+16098517579	OKTA	ACTIVE	03/14/2024 07:50 PM		۲		
	Google Authenticator	dizzy0	GOOGLE	PENDING_ACTIVATION	03/20/2024 01:45 PM		€		
			1	tems per page: 10 👻	1-3 of 3		<	>	
	Ä	_							

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  $\it{MFA}$  tab.

User Guide Version 1.09

- 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.
- 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. <sup>36</sup>

### 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.

- 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.

Identity Management (IDM)

 $<sup>^{36}</sup>$  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. window appears.

The Remove MFA Device

 $\bigcirc$ 

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. <sup>37</sup>

## 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.

 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.

User Guide Version 1.09

Identity Management (IDM)

**Commented [A1]:** Needs formatting w/ section #s - not sure if that will pop up when TT are accepted



 $<sup>^{37}</sup>$  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.

a lunana

The Update E-mail Address button appears under the "Actions"

column.

Ē	Ē	
---	---	--

- 3) Select the **Update E-Mail Address** button For the desired user. The Update E-Mail Address window appears. This button is also present in the User Details window the MFA tab under the "Actions" column.
- 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.

- 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.



 Select the *Reset Password* button window appears. for the desired user. The Reset Password

4) Select the "E-Mail a Password Reset link to the User" option and enter a justification.

Identity Management (IDM)

Get User Status

 Select the *Submit* button. The system displays a message which indicates the operation completed successfully. <sup>38</sup> <sup>39</sup>

## 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.

- 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.
- (Application Search Users Only) Select the *Get User Status* button. The *Reset Password* button appears under the "Actions" column.
  - <del>کت</del>
- 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. <sup>40</sup>
- Select the *Close* button. The system displays a message which indicates the operation completed successfully. <sup>41</sup> 42

<sup>&</sup>lt;sup>38</sup> 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.

<sup>&</sup>lt;sup>39</sup> The Reset Password hyperlink expires after four hours have elapsed. The user will be required to repeat this entire procedure if the link expires.

 $<sup>^{40}</sup>$  Help Desk Users bear the responsibility to properly authenticate the end user before giving them the temporary password.

<sup>&</sup>lt;sup>41</sup> 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.

<sup>&</sup>lt;sup>42</sup> The user is required to change their password when they sign into the system.

## 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". Get User Status 2) (Application Search Users Only) Select the Get User Status button. The Unlock Account button appears under the "Actions" column. for the desired user. The Unlock Account 3) Select the Unlock Account button 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.

How to Unlock a User's Account

**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.

 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.

Get	User Status
	over otatae

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

User Guide Version 1.09

Account window appears.



for the desired user. The Suspend

- 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

User Guide Version 1.09

 $<sup>^{\</sup>rm 43}$  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.

 $<sup>^{44}</sup>$  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 Get User Status 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. <sup>46</sup> $^{45}$ 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.

User Guide Version 1.09

- 5) Use the *LOA* menu to select the updated LOA. <sup>47</sup>
- 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.

 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 Unsuspend Account window appears. for the suspended user. The

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** 

<sup>&</sup>lt;sup>47</sup> A user's LOA can only be raised; it cannot be lowered.

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

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

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

The User Audit Search form appears.

Search	
User Audit Search	* Optional fields are labeled as (Optional).
Enterprise Search User Audit Role Request	Audit
User Audit Search requires both User ID and Event Type to p	erform a search.
User ID	Event Type
Requested Date Filter	
Last 7 Days	
O Last 30 Days	
O Last 60 Days	
O Date Range	
Clear Fields	User Audit

Figure 55: Help Desk User Audit Search Form

User Audit

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

The screen refreshes and the report

Search Results									
User Audit Search Results (Event Type - User Profile) Back to Search									
Total Results: 7 Filter									
User ID	Event Created By	Event Description	Timestamp	Old Value	New Value				
JOHNENDUSER2	JOHNENDUSER2	Company Address Line1	03/08/2021 02:13 PM		123 Business Street				
JOHNENDUSER2	JOHNENDUSER2	Company City	03/08/2021 02:13 PM		Podunk				
JOHNENDUSER2	JOHNENDUSER2	Company Name	03/08/2021 02:13 PM		Affluent HC				
JOHNENDUSER2	JOHNENDUSER2	Company Phone	03/08/2021 02:13 PM		216-657-4309				
JOHNENDUSER2	JOHNENDUSER2	Company State	03/08/2021 02:13 PM		MD				
JOHNENDUSER2	JOHNENDUSER2	Company Zip	03/08/2021 02:13 PM		12345				
JOHNENDUSER2	JOHNENDUSER2	Office Phone	03/08/2021 02:13 PM		216-657-4310				

Figure 56: User Audit Report - User Profile Events

Search Results	_						
User Audit Search Results (Event Type - User Authentication) Back to							
Total Results: 1		Filt	ter		٩		
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 Aud	dit Search	Results (Ever	nt Type -User Acce	ess)			Back to Search
Total Re:	esults: 26			Filter			٥
User ID		Event Description	Timestamp	Application	Role	Attribute Name	Attribute Value
JOHNAPPRO	OVERONE	Remove	03/16/2021 10:53 AM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Maryland
JOHNAPPRO	OVERONE	Remove	03/16/2021 10:53 AM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Kentucky
JOHNAPPRO	OVERONE	Remove	03/16/2021 10:53 AM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Massachusetts
JOHNAPPRO	OVERONE	Remove	05/25/2021 05:51 PM	Connexion	Connexion Authorizer	N/A	N/A
JOHNAPPRO	OVERONE	Certified	05/24/2021 12:21 PM	BCRS Web	BCRS CMS/CAA	N/A	N/A
JOHNAPPRO	OVERONE	Revoked	05/25/2021 05:12 PM	Connexion	Connexion Authorizer	N/A	N/A
				< 1 2 3 >		Results 10	s Per Page (Optional) X +

Figure 58: User Audit Report - User Access Events

- JOHNAPPROVERONE
- 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.

#### Back to Results

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

The search results window

## CMS XLC

## 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.

Help Desk Users. Col	o create Role Request Audit reports is or nsequently, audit report creation buttons o m of Application (Tier 1) Help Desk Users	do not appear on the
, ,	Desk/Manage Users button as describe Functions. The Enterprise Search form a	
2) Select the <b>Role</b> Search form ap	Role Request Audit button.	The Role Request Audit
	Search Results	_
	Request Audit Search * Optional fields are labeled as (	Optional).
	Enterprise Search User Audit Role Request Audit	
	Role Request Audit Search requires at least the User ID or Request ID to perform a search.	
	User ID (Optional)     Request ID (Optional)	
	Requested Date Filter	
	<ul> <li>Last 7 Days</li> </ul>	
	Last 30 Days	
	Date Range	
	Clear Fields Role Reque	st Audit
		_
-		
F	igure 59: Help Desk Role Request Audit Se	arch Form
3) Enter a User ID	or enter a Request ID.	

4) Select a Date Range.

Role Request Audit

5) Select the *Role Request Audit* button. report appears on the Results tab.

The screen refreshes and the

User Guide Version 1.09

Role Request Audit Results Back to Sea								to Search	
Total Results	: 13				Filte	r			Q
User ID	Request ID	Requested By	Туре	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
				ŀ	< 1 2	2 3 >	ſ	- Results Per Pag 5	e (Optional) – × •

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.

Back to Results

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.

 $<sup>^{48}</sup>$  If the Application is not already an IDM integrated application, the Application Team/Owner also opens an IDM Jira ticket.

 $<sup>^{\</sup>rm 49}$  The IDM SR process is described on the IDM Confluence page: https://confluenceent.cms.gov/pages/viewpage.action?spaceKey=IDM&title=Service+Request+Proce ss+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.
- The Application Users add the YubiKey MFA device to their account using the procedure in Section 0 How to Add a YubiKey MFA Device. <sup>50</sup>

**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.

User Guide Version 1.09

 $<sup>^{50}</sup>$  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.

<sup>&</sup>lt;sup>51</sup> The YubiKey Personalization Tool is available for download from the Yubico website: <u>https://www.yubico.com/support/download/yubikey-personalization-tools/</u>

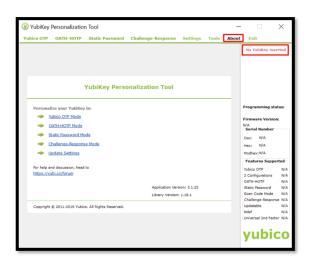


Figure 61: YubiKey Personalization Tool Startup Window

- 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.

W YubiKey Personalization Tool	- 🗆 )	×
Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Tools About	Exit	
YubiKey Personalization Tool	YubiRey is insert	ed
Personalize your Yubikey in: Yubico OTP Mode OXTL+HOTP Mode	Programming statu Slot 1 and 2 configur Firmware Version: 4.4.5 Serial Number	
Static Password Mode     Challenge Resource Mode     Update Settings	Dec: 12447200 Hex: bdede0 Modhex: ntutuc	
Ro help and discussion, head to https://www.conforcum Application Version: 3.1.25	Features Support Yubico OTP 2 Configurations OATH-HOTP Static Password	ed * * *
Library Version: 1.18.1 Copyright © 2011-2016 Yubico. All Rights Reserved.	Scan Code Mode Challenge-Response Updatable Ndef Universal 2nd Factor	5 5 5 <b>X</b> 5

Figure 62: YubiKey Personalization Tool - Device Present

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

User Guide Version 1.09

98

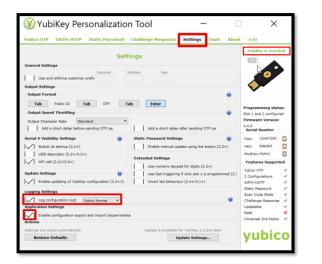


Figure 63: YubiKey Personalization Tool - Settings Tab

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

Program	n in Yu	bico O1	rP m	iode - A	dvanced			YubiKey is insert	ed
Configuration Slot Select the configuration slot to be pro Configuration Slot 1		figuration Si	ot 2				0		
Program Multiple YubiKeys			Conf	iguration Pr	rotection (6 by	tes Hex)		•	
Automatically program YubiKeys	when insert	red	nutio	Cey(s) unprol	tected - Keep it !	that way			
Parameter Generation Scheme				Int Access Co Use Serial Nu				Programming state Slot 1 and 2 configur	
Identity from serial; Randomize Seco	rets			Use Senal Nu Access Code	mber			Firmware Version:	
Yubico OTP Parameters				Jse Serial Nu	mber			4.4.5 Serial Number	
Public Identity (1-16 bytes Modh	ex cc cc cc	nt ut uc	_			Generate		Dec: 12447200	E
Public Identity Length	6 🗘	(5 bytes is d	efault i	ingth as requ	ired by Yubica	OTP validation serv	er)	Hex: bdede0	0
V Private Identity (6 bytes Hex)	00 00 00	00 00 00				Generate		Modhex: ntutuc	Ľ
Secret Key (16 bytes Hex)	00 00 00	0 00 00 00 0	00 00	00 00 00 00	00 00 00	Generate	0	Features Support	ed
Actions								Yubico OTP	2
Press Write Configuration button to	program yo	ur YubiKey's	pelectr	ed configurat	ion slet			2 Configurations OATH-HOTP	1
Write Configuration	Stop	Reset		Back		Export		Static Password	
								Scan Code Mode	1
Results								Challenge-Response Updatable	1
# Public Identity (Modhex)	Status	Timestamp	6				~	Ndef	
								Universal 2nd Fector	

Figure 64: YubiKey Personalization Tool - Yubico OTP Tab

User Guide Version 1.09

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

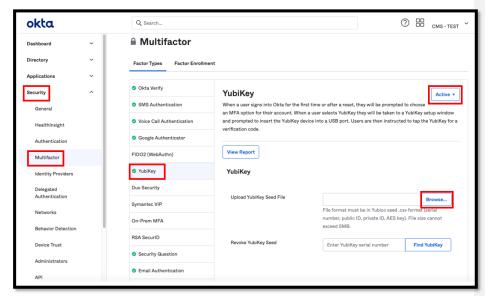


Figure 65: Okta YubiKey Administration Window

User Guide Version 1.09

- 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.
- 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).
- Enter the YubiKey serial number into the *Revoke YubiKey Seed* field then select the *Find YubiKey* button.
- 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 <u>not</u> 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

	Арр	lication Search	Ente	rprise Search		
	Application Help Desk	Application Approver	IDM Help Desk	Application Help Desk	Application Approver	IDM Help Desk
Remove Multiple Roles/Attributes	0	0				х
Export Results		Х				
View User Details	Х	Х		Х		Х
Update LOA	0			0		Х
Lock Account						Х
Unlock Account				Х		Х
Enable User						Х
Disable User						Х
Reset Password (Email)				Х		х
Reset Password (Manual)				0		х
Manage MFA Device	Х		Х	Х		Х
Remove Roles/Attributes		0				х
Promote User						

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

<sup>53</sup> The IDM SR process is described on the IDM Confluence page: <u>https://confluenceent.cms.gov/pages/viewpage.action?spaceKey=IDM&title=Service+Request+Proce</u> <u>ss+for+IDM</u>

# 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)

User Guide Version 1.09

Identity Management (IDM)

Appendix E: Acronyms

# 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	

CMS XLC

Identity Management (IDM)