CMS Enterprise Identity Management (EIDM)

Help Desk User Guide

Working Copy Version 0.7 Release 16 Final

Note: Working Copy versions delivered to the client for review will be published as a Major Version.

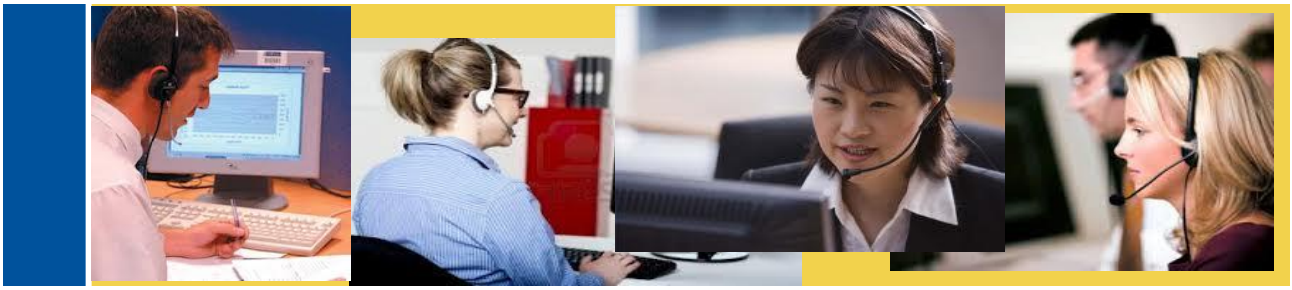
Client has agreed to review these documents as as-is, ongoing, “work-in-process” drafts and working copy versions.

Revision: April 2017

This page is intentionally blank.

Table of Contents

List of Tables



EIDM Help Desk User Guide

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 provides funds and guidance for all of the 50 states in the nation, for their Medicaid programs and Children's Health Insurance Program (CHIP). CMS works together with the CMS community and organizations in delivering improved and better coordinated care.

What is EIDM?

CMS has established the Enterprise Identity Management (EIDM) website to provide our Business Partners with a means to apply for, obtain approval, and receive a single User ID they can use to access one or more CMS applications.

What is the "EIDM Help Desk User Guide"?

The "EIDM Help Desk User Guide" is for individuals who have an Application Help Desk User role. This guide provides basic step-by-step instructions on how to manage users and perform various Help Desk functions.

System Users

EIDM system users fall into the following role types:

- **End Users**: users who register with EIDM for access to CMS applications
- **Application Help Desk Users**: users who provide Tier 1 Help Desk support for End Users (e.g., Unlock Account or Reset Password)
- **Application Approvers**: users who approve End User role requests
  Note: In some applications, Application Help Desk Users act as Approvers who are responsible for approving End User and/or Approver role requests.
- **EIDM Help Desk Users**: users who provide Tier 2 Help Desk support for all EIDM-integrated application users (e.g., Enable User or Lock Account)
- **Authorizers**: users who are responsible for approving Approver or Help Desk User role requests.

These users may access the system by navigating to the CMS Enterprise Portal (portal.cms.gov), registering for an EIDM account, and then logging into the portal with their EIDM account. Within the portal, they can access the Help Desk interface and use it to perform actions such as resetting passwords, unlocking accounts, and disabling users.

Help Desk Privileges

Depending on the user's rights and permissions, the EIDM Help Desk interface has two different search options. These options include:

- **Application Search**: a type of search that allows Help Desk Users and Approvers to search and manage accounts for users with a role in their application(s)
- **Enterprise Search**: a type of search that allows Application Help Desk Users to search and manage accounts for users who do not have a role (e.g., helping users who called the wrong Help Desk or updating the LOA of a user who is attempting to request a role within the application supported by the Help Desk user)

Help Desk Users and Approvers have different privileges depending on whether they are accessing user accounts through the 'Application Search' or 'Enterprise Search'. The following table outlines each role's privileges:

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

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

Table 1: Help Desk Privileges

Help Desk privileges have the following limitations:

- The 'Promote User' function is only available for organization-based applications.
- When a user has a 'Disabled' status:
  - Application Help Desk Users and Application Approvers can only view the user's details.
  - EIDM Help Desk Users can only view the user's details or access the 'Enable User' function.
- All Help Desk privileges are accessible through the 'My Helpdesk' or 'View and Manage Users' link.
- With the exception of 'Update LOA', all Help Desk privileges are available on the search results and 'User Details' pages; the 'Update LOA' function is only accessible on the 'User Details' page.

2. Before You Begin

Before accessing the application, consider certain computer settings to ensure it functions properly.

To optimize your EIDM system access, check the following items:

1. **Screen Resolution**: CMS screens are designed to be viewed at a minimum resolution of 800 x 600. Your resolution is the number of pixels your monitor displays horizontally and vertically and is generally expressed as width times height (e.g., 800 pixels wide x 600 pixels high or 800 x 600). The more pixels that display, the better your on-screen text and images will look.
2. **Plug-Ins**: Verify that your computer has the latest version of JAVA and ActiveX installed.

Note
Verify the latest versions of JAVA or ActiveX by going to the JAVA website (www.java.com) and Adobe website (www.adobe.com), or by contacting your internal IT Help Desk.

3. **Pop-up Blockers**: Verify that your browser's pop-up blockers are disabled.
4. **Supported Browsers**: EIDM supports Internet Explorer 11, Firefox, Google Chrome, and Safari.

As part of getting started in the Help Desk interface, please review the following procedures:

1. **Verify your Computer Settings**
2. **Register for a CMS Enterprise Portal Account** *(refer to the "CMS EIDM User Guide")*
3. **Log into the CMS Enterprise Portal**
4. **Add a Help Desk Role** *(refer to the "CMS EIDM User Guide")*
5. Access the Help Desk **using either the 'My Helpdesk' or 'View and Manage Users' link**

If needed, please refer to the "CMS EIDM User Guide" for how to access EIDM in 508 Accessibility Mode.

Verify Your Computer Settings

This section outlines the steps to verify your computer settings.

	Action
Step 1	Verify your screen resolution. **Windows 7 and 8:** Select the **Start** button, select **Control Panel**, find **Appearance and Personalization**, and select **Adjust Screen Resolution**. Ensure the correct monitor is selected in the **Display** drop-down list. Below that list, the **Resolution** drop-down list displays your setting. Note this setting and select **Cancel** to leave your settings as they are.
Step 2	Install the latest version of JAVA and ActiveX. **JAVA:** Open your browser, navigate to java.com, select **Free Java Download**, select **Agree and Start Free Download**, open the download, accept the terms, and select **Install**, select **Next**, wait for the program to install, and select **Close**.

	Action
	ActiveX: Open your browser, navigate to get.adobe.com/flashplayer, select **Adobe® Flash® Player system plug-in**, select **Install Now**, open the download, select **Run**, accept the terms, and select **Next**, wait for the program to install, and select **Finish**.
Step 3	Disable you browser's pop-up blockers.
	Internet Explorer 11: Open your browser, select the **Tools** icon, select **Internet options**, open the **Privacy** tab, uncheck the **Turn on Pop-up blocker** checkbox, and select **OK**.
	Firefox: Open your browser, select the **Menu** icon, select **Content** in the navigation pane, find the **Pop-ups** section, and uncheck the **Block Pop-up windows** checkbox.
	Chrome: Open your browser, select the **Menu** icon, select **Settings**, select **Show Advanced Settings**, find the **Privacy** section, select **Content Settings**, find the **Pop-Ups** section, select **Allow all sites to show pop-ups**, and select **Done**.
	Safari: Open your browser, select the **Safari** button, select **Preferences**, open the **Security** tab, find the **Web content** section, and uncheck the **Block pop-up windows** checkbox.

Log into the CMS Enterprise Portal

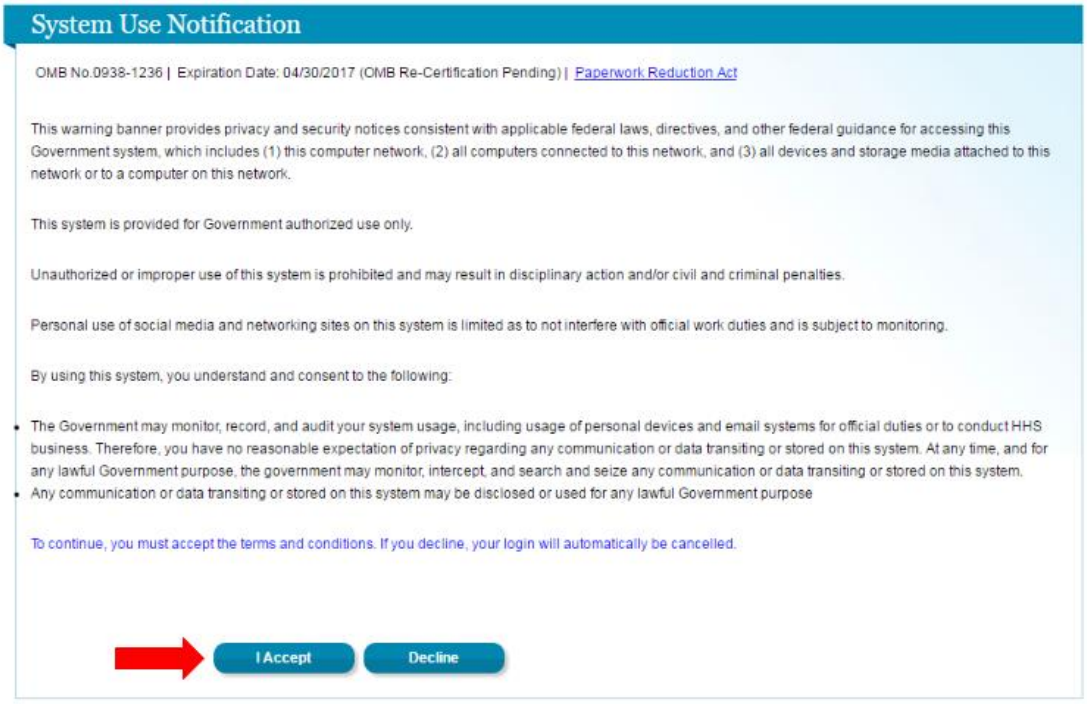
This section outlines the steps to log into the CMS Enterprise Portal.

Important Notes
If you do not have an EIDM User ID and Password or an application role, refer to the "CMS EIDM User Guide" for details on how to register in EIDM to create your User ID and request a role.

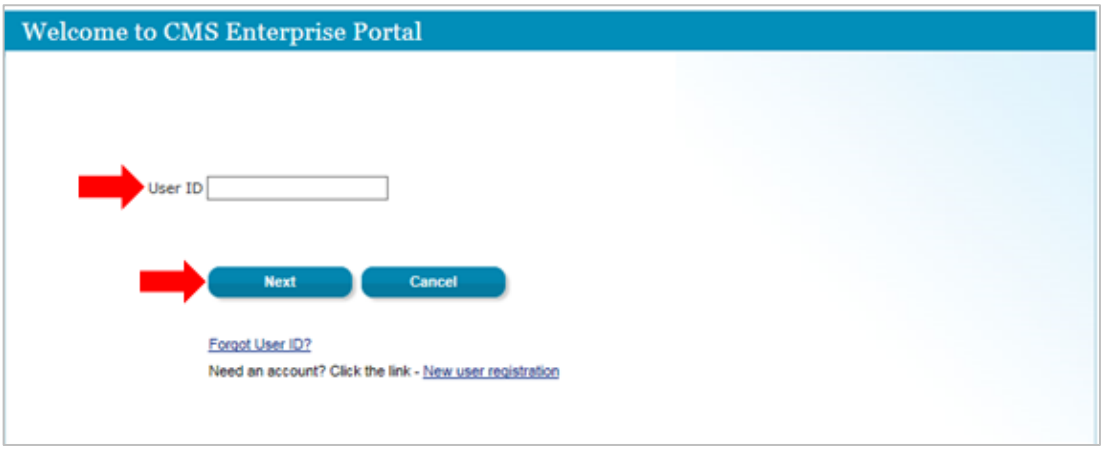
	Action
Step 1	Navigate to the CMS Enterprise Portal (portal.cms.gov) and select **Login to CMS Secure Portal**.

Step 2	Read the terms and conditions and select **I Accept**.

Action



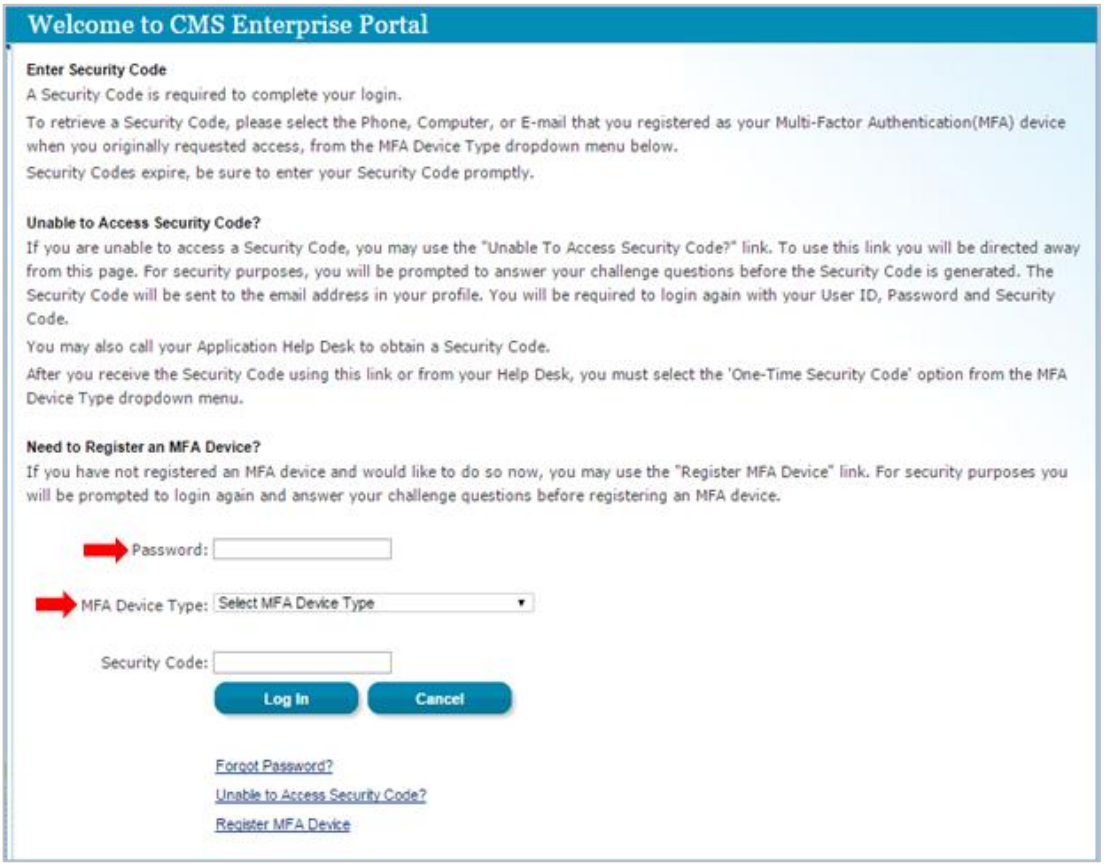
Step 3 Enter your **User ID** and select **Next**.



Step 4 Enter your **Password** and select the **MFA Device Type** for the Multi-Factor Authentication

Action

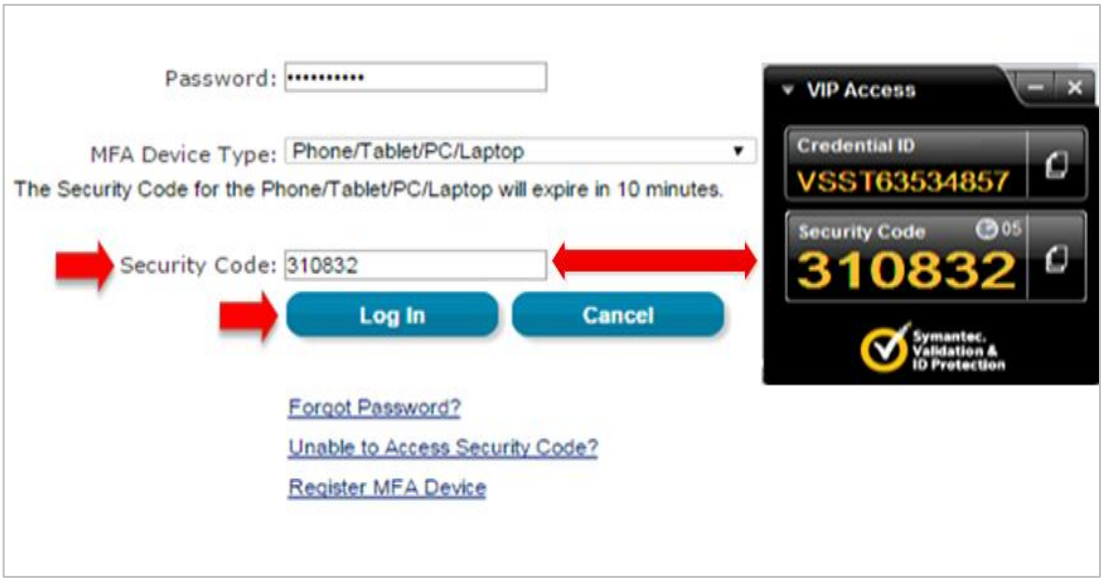
(MFA) device you registered.



Action	
Step 5	If your **MFA Device Type** is **Phone/Tablet/PC/Laptop**, enter the **Security Code** from your Symantec VIP Access application and select **Log In**.

Note

If you registered a different device, skip to **Step 6**.

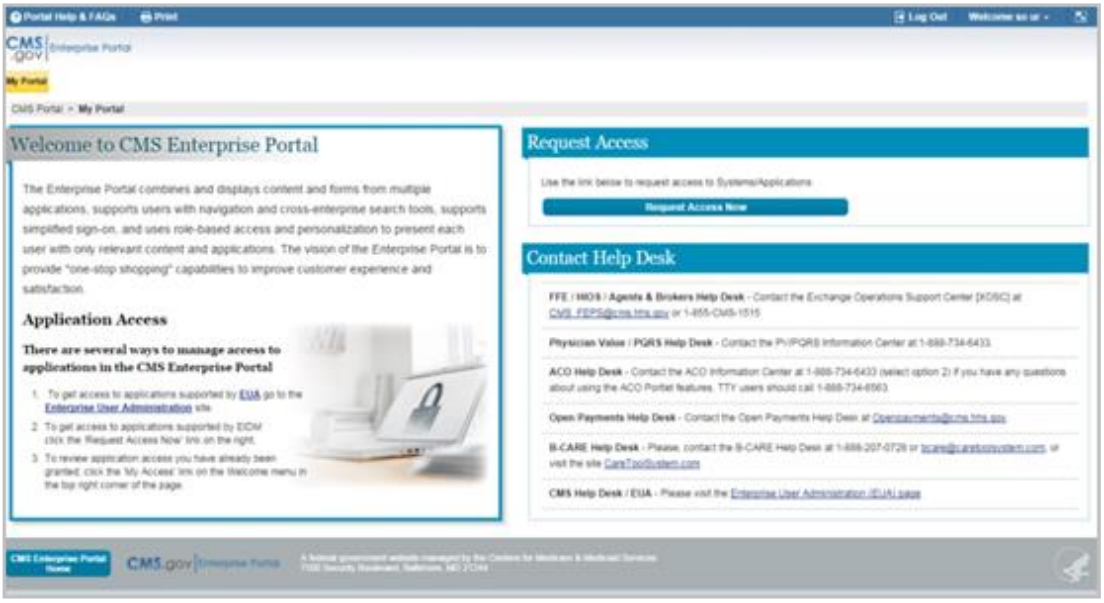


Step 6	If your **MFA Device Type** is **Text Message (SMS)**, **E-Mail**, or **Interactive Voice Response (IVR)**, select **Send**, enter the **Security Code** your device receives, and select **Log In**.

Note

The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires in 30 minutes. The 'Security Code' for the other MFA device types expires in 10 minutes. If you are unable to enter the code within the allotted period, you must request a new one.

Action	
Step 7	The system displays the **Welcome to CMS Enterprise Portal** page.



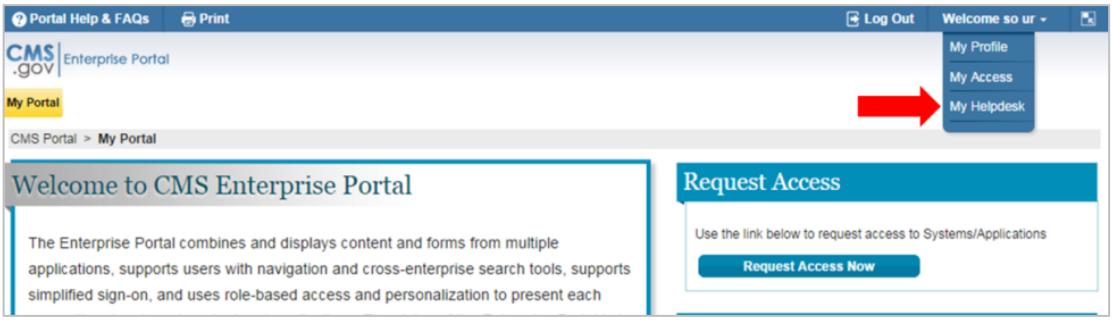
Access the Help Desk via 'My Helpdesk'

This section outlines the steps to access the Help Desk interface using the 'My Helpdesk' link.

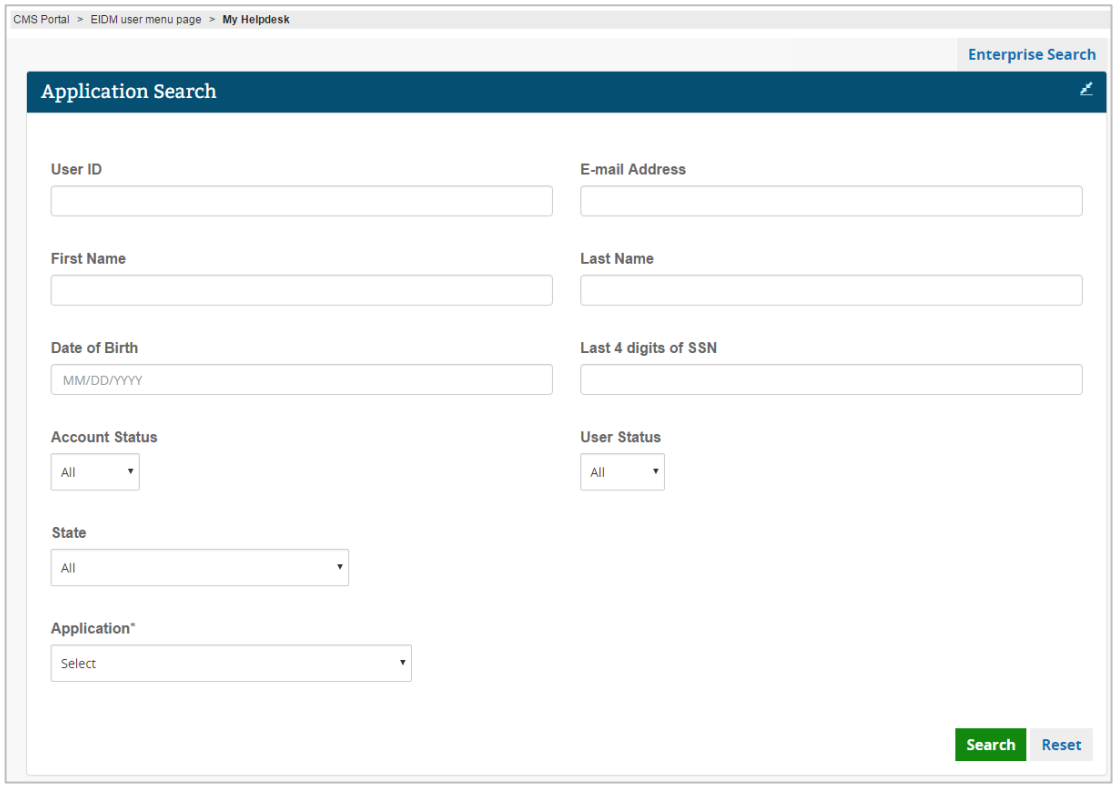
	Action
Step 1	Log into the CMS Enterprise Portal.
Step 2	Locate the **Welcome <First Name> <Last Name>** drop-down list at the top-right corner of the page and select **My Helpdesk**.

Note

Alternatively, select **Request Access Now** in the 'Request Access' section.



Step 3 The EIDM Help Desk interface displays and allows you to search for a user.



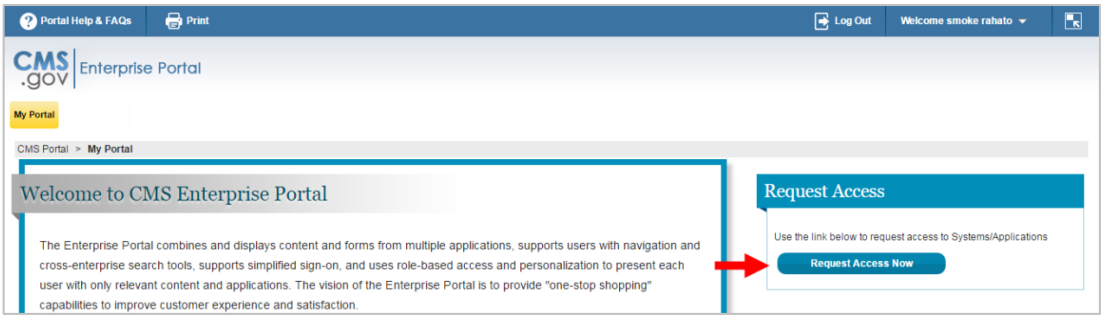
Access the Help Desk via 'View and Manage Users'

This section outlines the steps to access the Help Desk interface using the 'View and Manage Users' link.

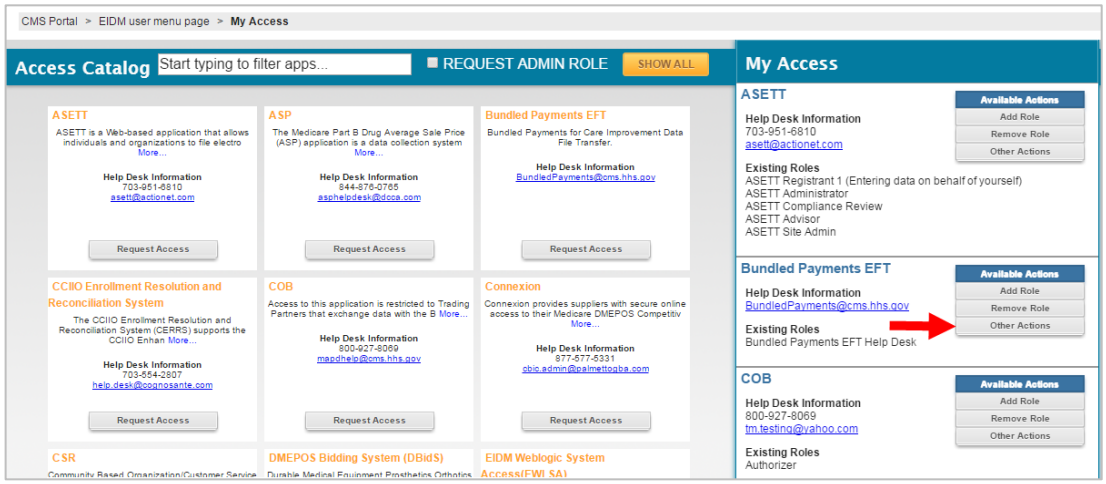
	Action
Step 1	Log into the CMS Enterprise Portal.
Step 2	Select **Request Access Now**.

Note

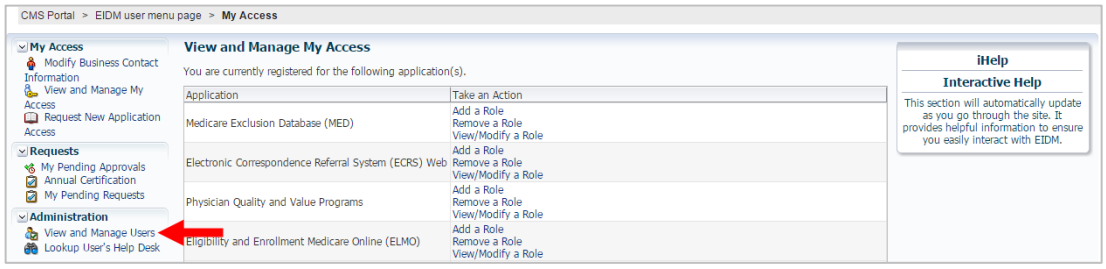
Alternatively, locate the **Welcome <First Name> <Last Name>** drop-down list at the top-right corner of the page and select **My Access**.



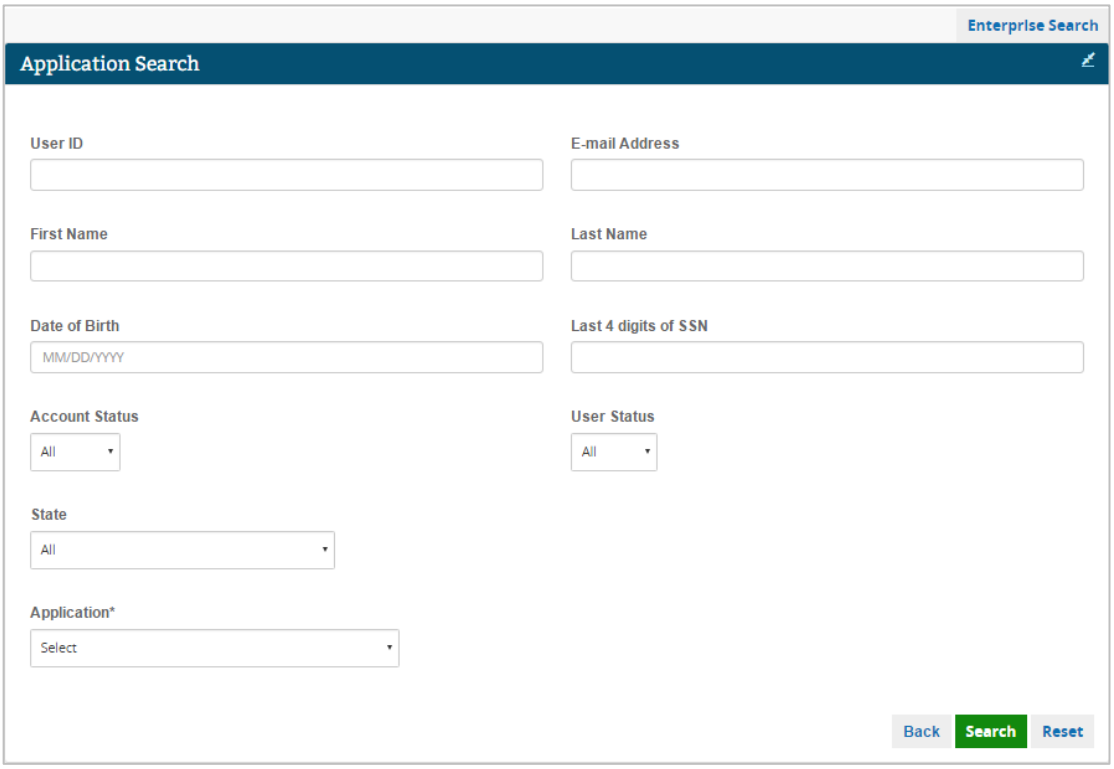
Step 3 Locate the 'My Access' section in the right pane and select **Other Actions**.



Step 4 Locate the 'Administration' section in the left pane and select **View and Manage Users**.



Action	
Step 5	The EIDM Help Desk interface displays and allows you to search for a user.



Note

For both 'Application Search' and 'Enterprise Search', select **Back** to return to the previous page.

3. Searching for a User

The Help Desk interface allows Application Help Desk Users to search for user accounts. Depending on your rights and permissions, the Help Desk interface may provide the following search options:

- Application Search
- Enterprise Search

Application Help Desk Users have the ability to use different criteria in each search option. The following table outlines each search's available criteria:

Feld	Application Search	Enterprise Search
User ID	✓	✓
E-mail Address	✓	✓
First Name	✓	✓
Last Name	✓	✓
Date of Birth	✓	✓
Last 4 Digits of SSN	✓	✓
State	✓	✓
Account Status	✓	✓
User Status	✓	✓
Application	✓	-
Group	✓	-
Role	✓	-
Role Attributes	✓	-

Table 2: Search Criteria

For both search options, the Help Desk interface has the following rules and restrictions in place:

- Enter at least two characters in a given field before selecting the 'Search' button.
- Search fields cannot contain the following special characters:
  - Ampersand (&)
  - Asterisk (*)
  - Cap sign (^)
  - Double Quotation Marks (")
  - Greater-than Sign (>)
  - Less-than Sign (<)
  - Percentage (%)
- **Application Search Only**: To search for a user, enter criteria in at least the 'Application' field.
- **Enterprise Search Only**: To search for a user, enter criteria in at least the 'First name' and 'Last name' (or) 'User ID '(or) 'E-mail Address' field(s).

Important Notes

- **ONLY ONE** Help Desk session should be open at any time. Trying to open multiple sessions will automatically log you out of the original session.
- **DO NOT** open the Help Desk interface in more than one tab or window in the same browser. You may time out in one tab/window, which will log you out of all tabs/windows.
- **DO NOT** use the 'Refresh' button on your browser; the system does not refresh the page as expected.

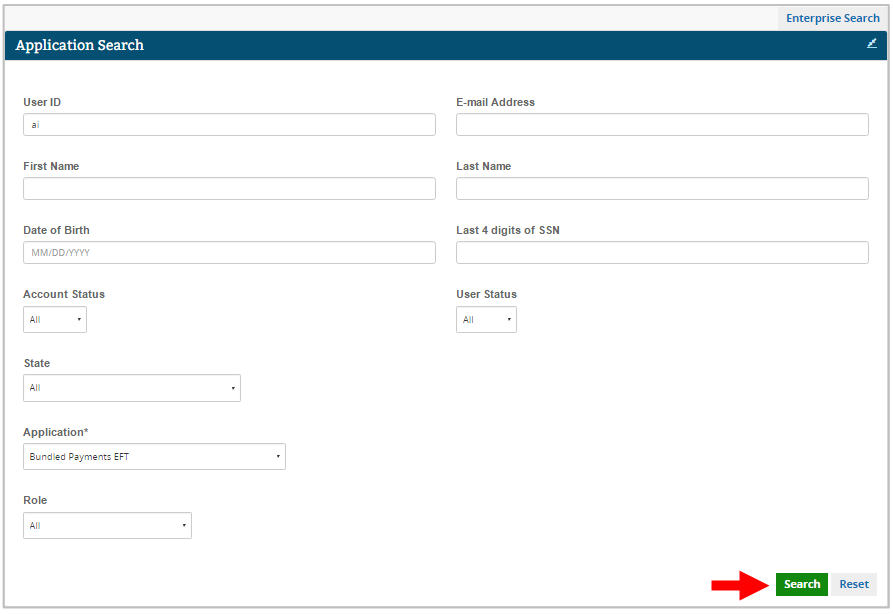
Application Search

The Help Desk interface's 'Application Search' is a type of search that allows Application Help Desk Users to search and manage accounts for users with a role in their application.

This section outlines the steps to perform an 'Application Search' within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User and access the Help Desk.

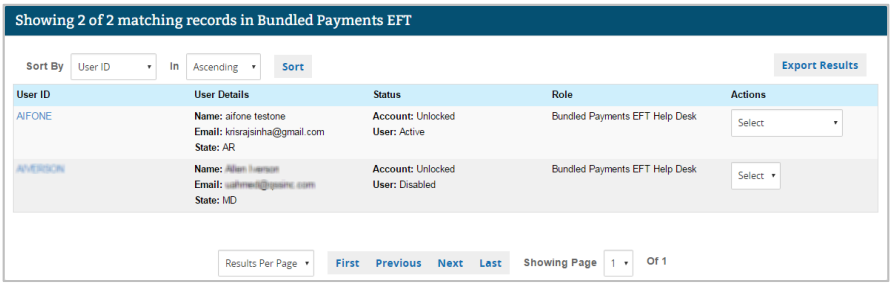
Step 2 The 'Application Search' criteria page displays. Enter at least the 'Application' to complete your criteria and select **Search**.



Note

If accessing 'Application Search' from 'View and Manage Users', select **Back** to return to the previous page.

Step 3 Up to the first 1,000 results display.



Note

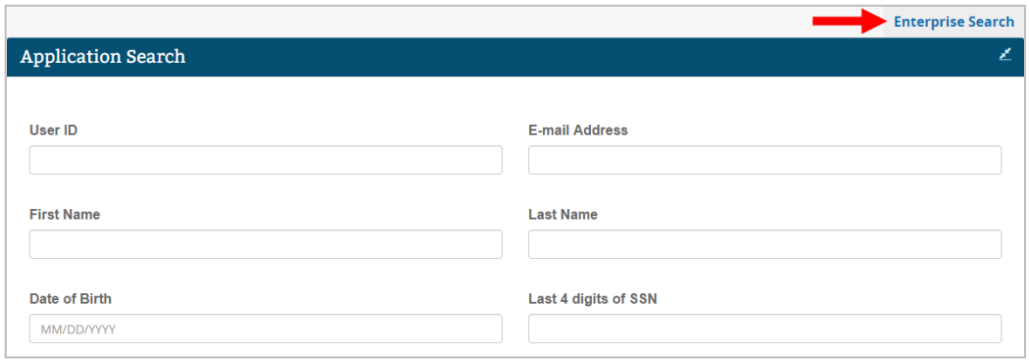
If performing an attribute-based search, the search results only display attribute values provided in the search criteria.

Enterprise Search

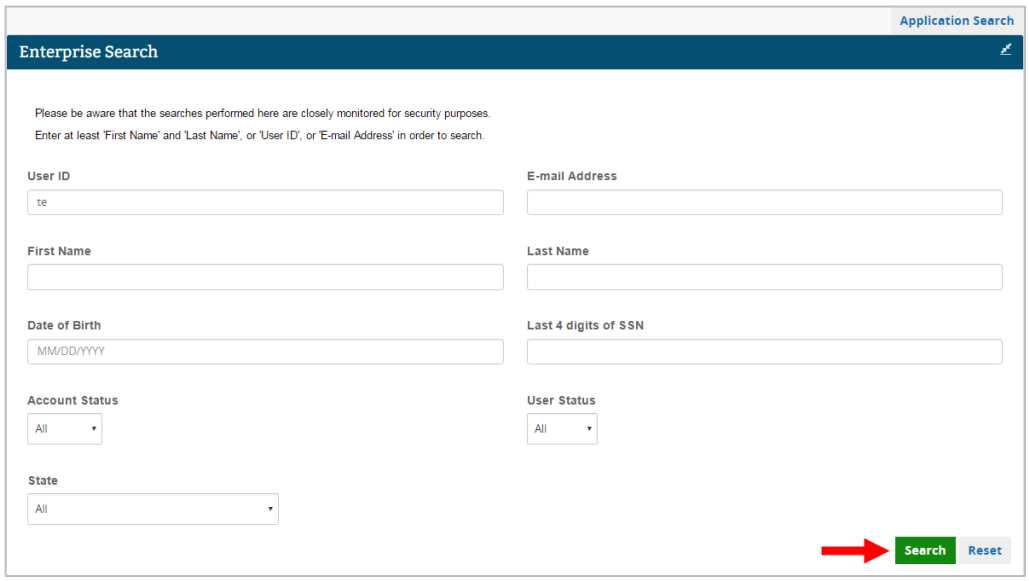
The Help Desk interface's 'Enterprise Search' is a type of search that allows Application Help Desk Users to search and manage accounts for users who do not have a role (e.g., helping users who called the wrong Help Desk or updating the LOA of a user who is attempting to request a role with the application supported by the Help Desk user).

This section outlines the steps to perform an 'Enterprise Search' within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User and access the Help Desk.
Step 2	The 'Application Search' criteria page displays. Select **Enterprise Search** in the top-right corner of the page.



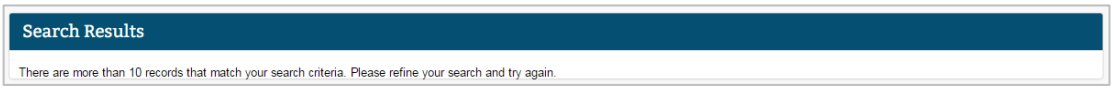
Step 3	The 'Enterprise Search' criteria page displays. Enter at least the 'User ID' (or) 'E-mail Address' (or) a combination of 'First Name' (and) 'Last Name' to complete your criteria and select **Search**.



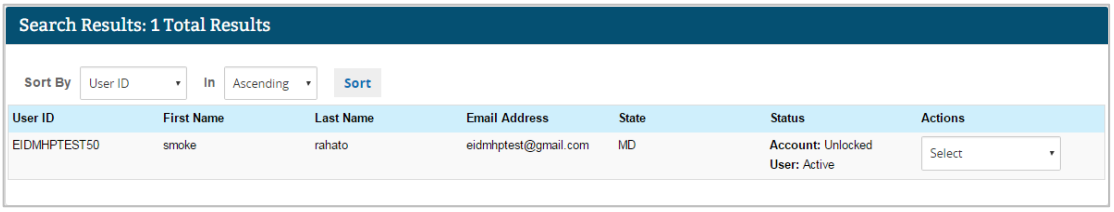
Note

If accessing 'Enterprise Search' from 'View and Manage Users', select Back to return to the previous page.

Action	
Step 4	If there are more than ten results, an error message displays.



Step 5 Once the search contains ten or less results, all the users matching the criteria displays.



4. Removing Multiple Users' Roles/Attributes

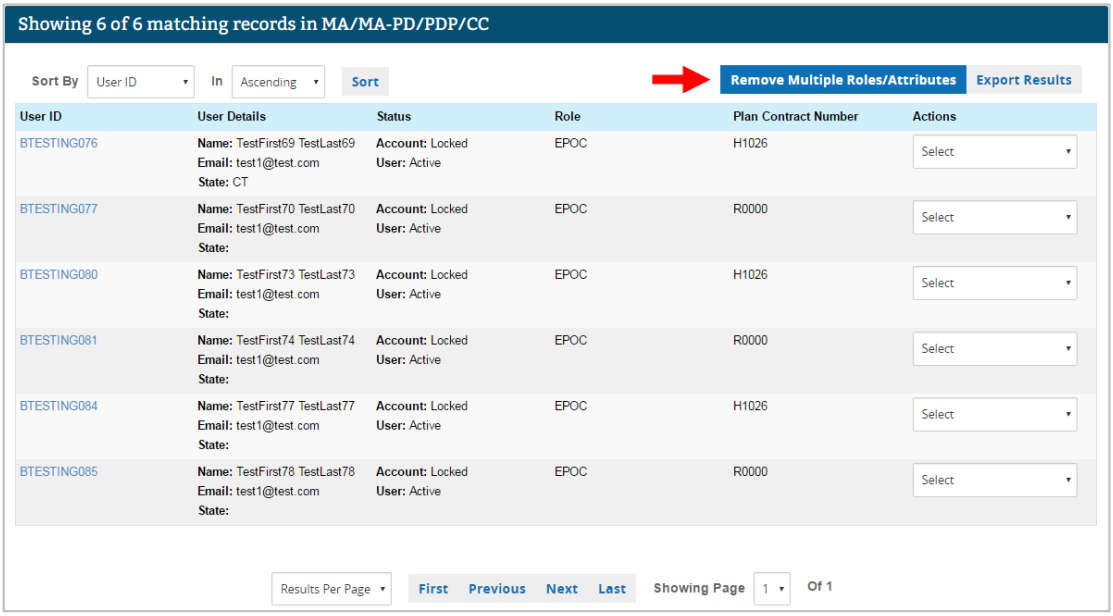
The Help Desk interface's 'Remove Multiple Roles/Attributes' function allows Application Help Desk Users to remove one or more roles or attributes from one or more users (i.e., bulk role/attribute removal). It is only accessible through the 'Application Search'.

Important Notes

- The 'Remove Multiple Roles/Attributes' function is optional and configurable by application. To configure this function for your application, please follow the process outlined in "Appendix A: Requesting Configurable Help Desk Privileges".
- Application Help Desk Users must select a role in the search criteria for the 'Remove Multiple Roles/Attributes' button to be available on the results page.

This section outlines the steps to perform a bulk removal within the EIDM system.

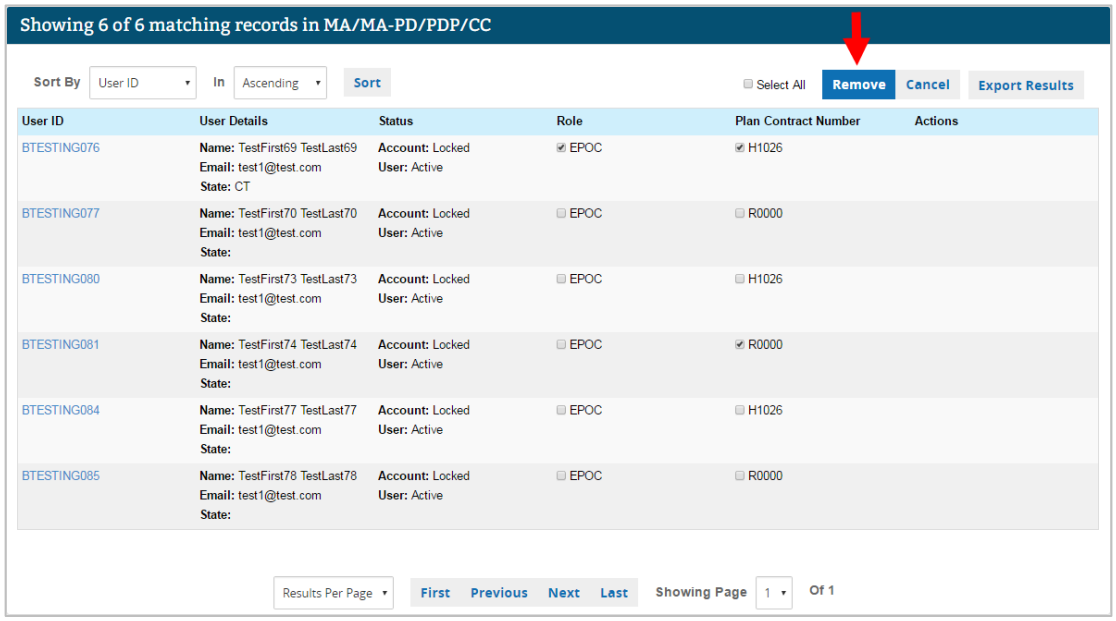
	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search'.
Step 2	Select **Remove Multiple Roles/Attributes** at the top of the search results.



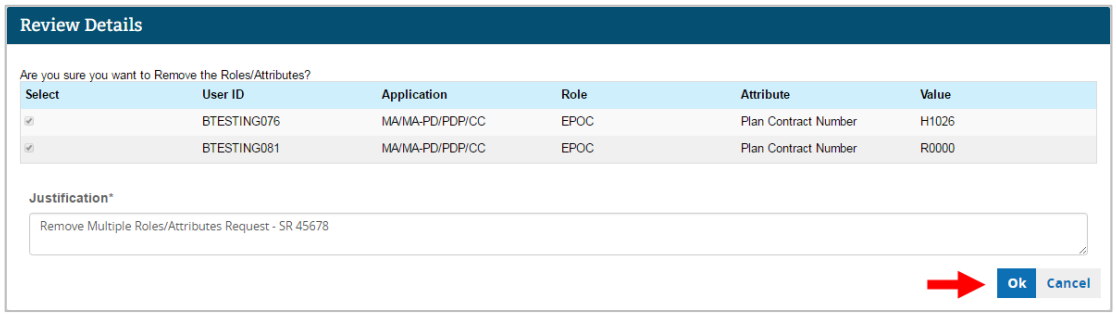
Action	
Step 3	The page updates to include checkboxes beside all roles and attributes and display the 'Select All' checkbox, 'Remove' button, and 'Cancel' button. Check the boxes for the roles/attributes you want to remove and select **Remove**.

Note

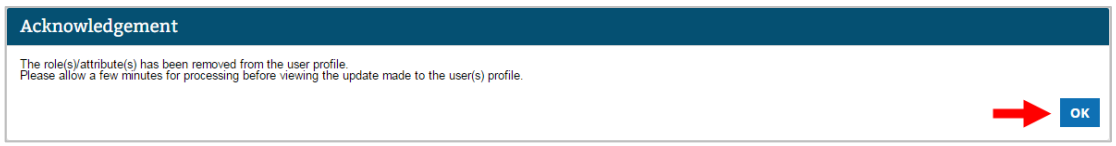
Once you remove these attributes, they cannot be restored; the user will have to request them again.



Step 4	The 'Review Details' page displays. Enter a **Justification** and select **OK**.



Step 5	A confirmation message displays. Select **OK**.

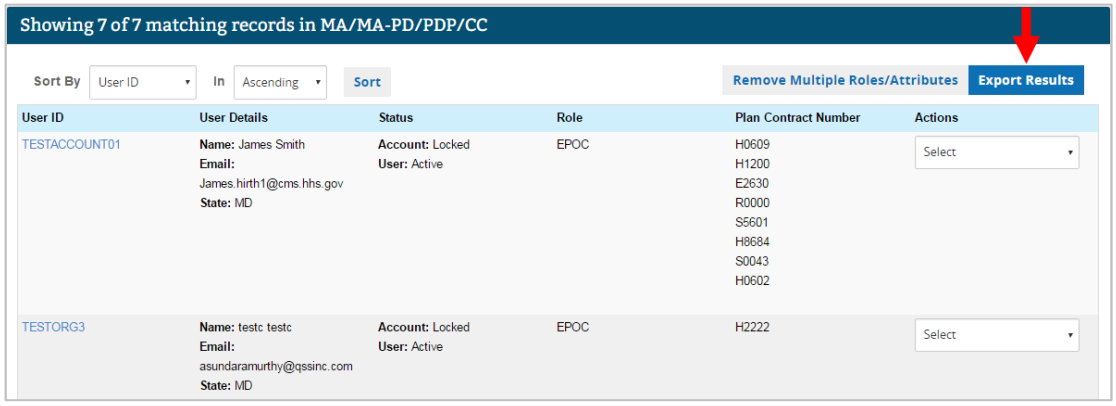


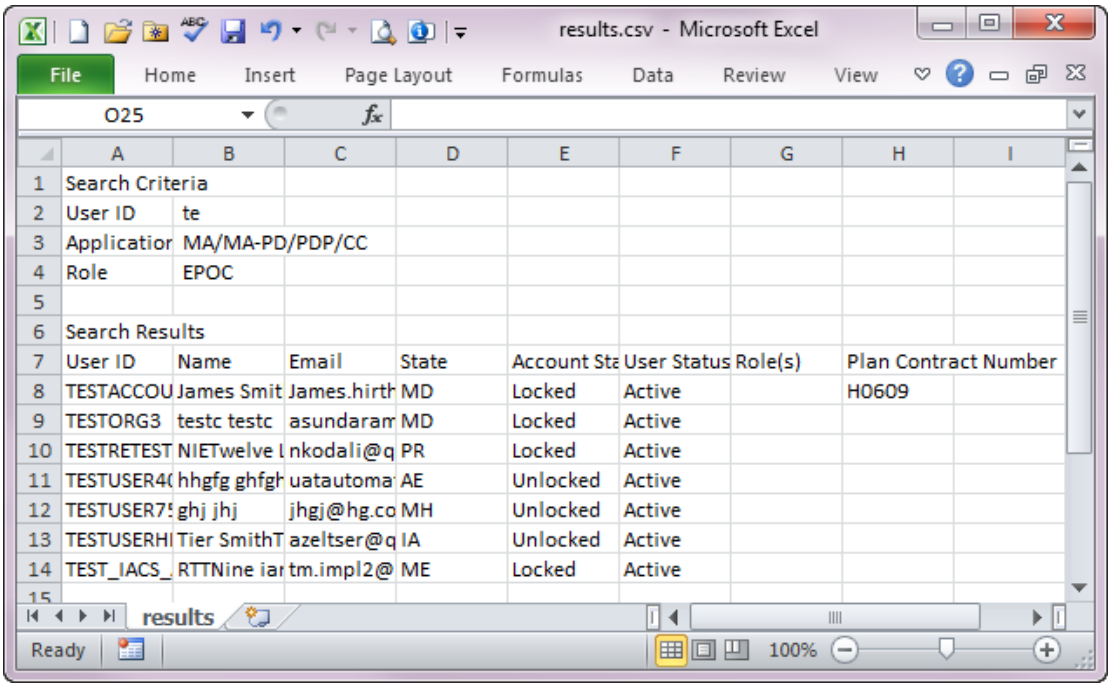
5. Exporting Results

The Help Desk interface's 'Export Results' function allows Application Help Desk Users to generate a Microsoft Excel Workbook (XLS) file containing their search results. It is only accessible through the 'Application Search'.

This section outlines the steps to export their 'Application Search' results to an XLS file in the EIDM system.

Action	
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search'.
Step 2	Select **Export Results** at the top of the search results.
Step 3	An XLS file generates. It contains a copy of the search criteria and results.



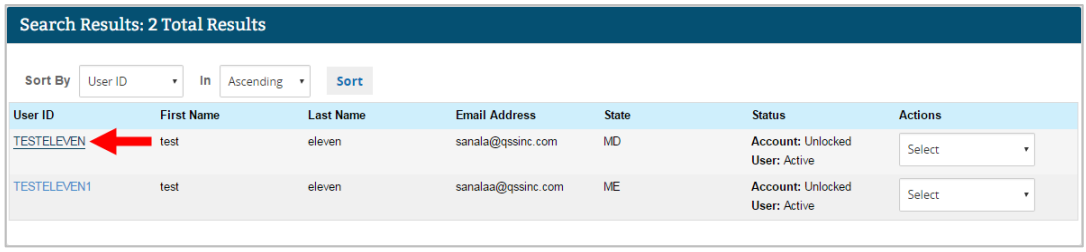


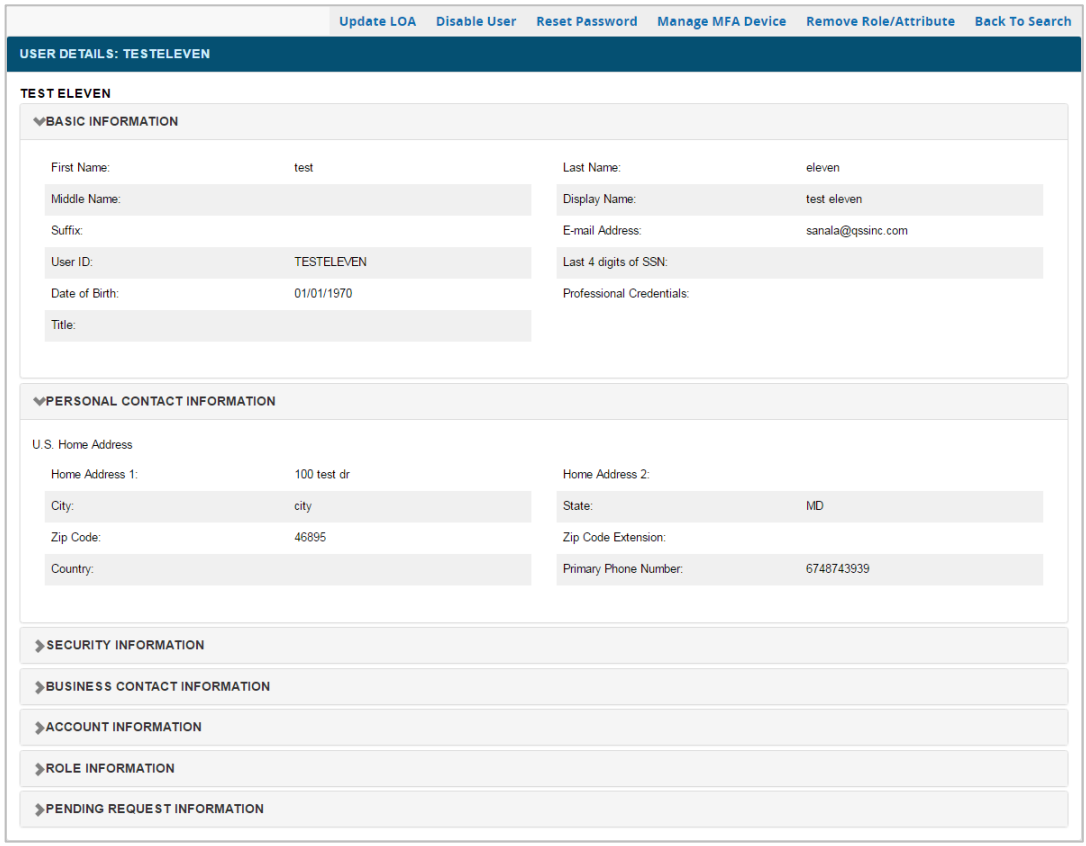
6. Viewing a User's Details

The Help Desk interface's 'User Details' function allows Application Help Desk Users to view a user's account information. It is accessible through both the 'Application Search' and 'Enterprise Search'.

This section outlines the steps to view a user's account information within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Access the user account you wish to view by selecting their ID link in the 'User ID' column.
Step 3	The 'User Details' page displays with the applicable details.





7. Cancelling a User's Pending Role Request

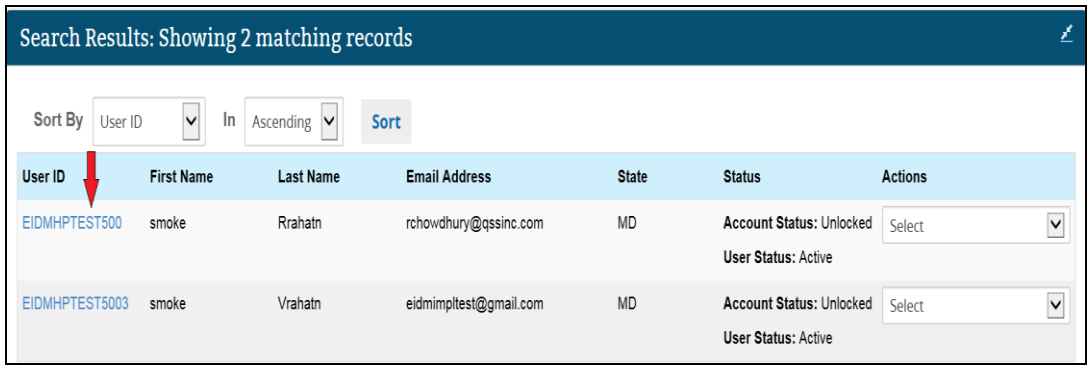
The Help Desk interface's 'Pending Request Information' function on the 'User Details' page allows Application Help Desk Users to view and cancel a user's pending role request. It is accessible through both 'Application Search' and 'Enterprise Search'.

Important Notes

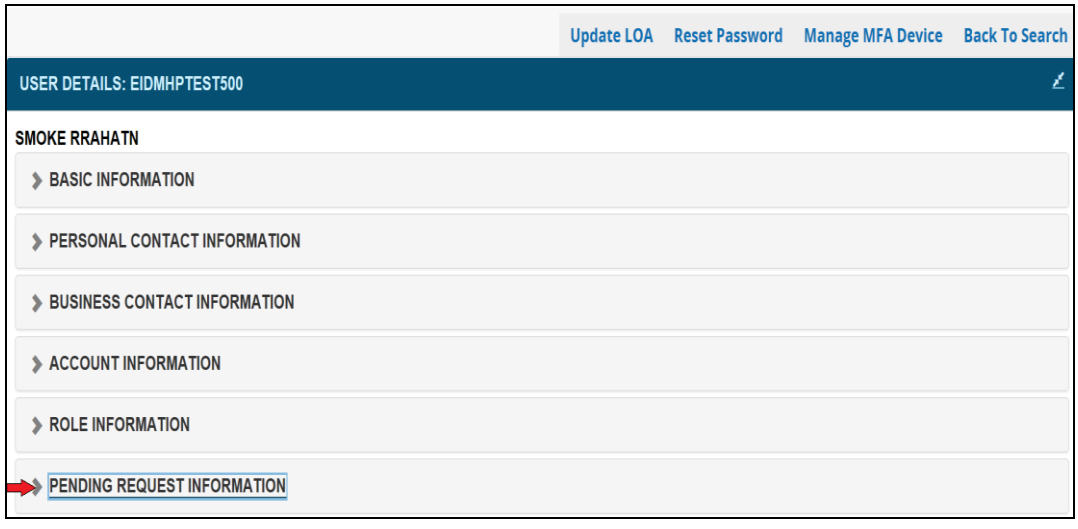
- The Application Help Desk will be able to cancel a user's role request related to their own application.
- The Application Help Desk will be able to search for users using Application Search only if the user already has a role in the application.

This section outlines the steps to cancel a user's pending role request within the EIDM system.

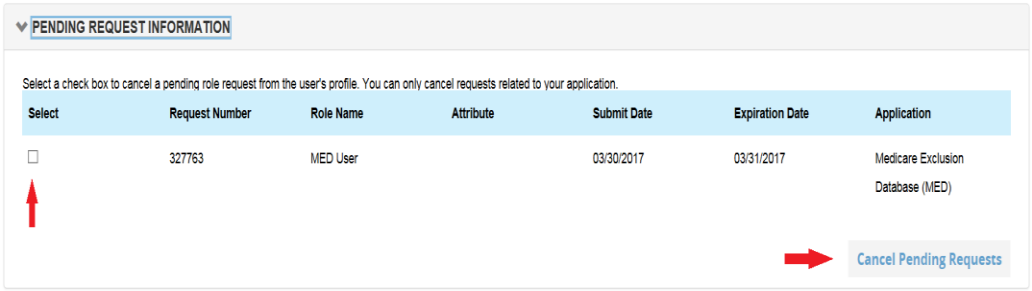
	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, perform an 'Application Search' or 'Enterprise Search'.



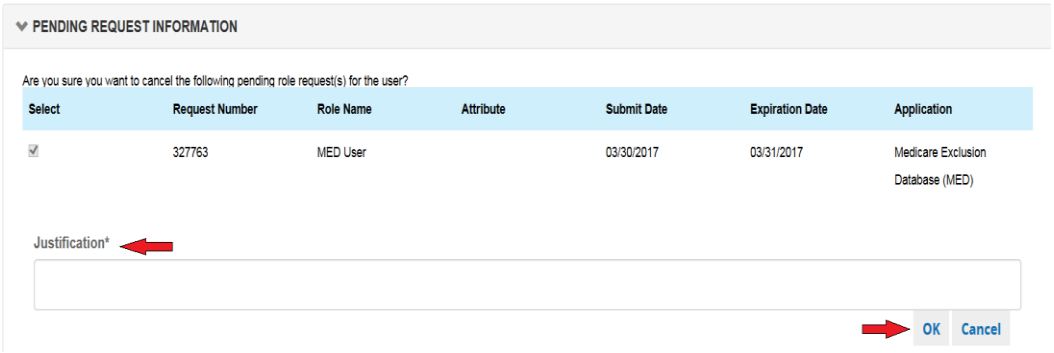
Step 2	Access the 'User Details' page for the user whose role request you wish to cancel, and select **Pending Request Information.**



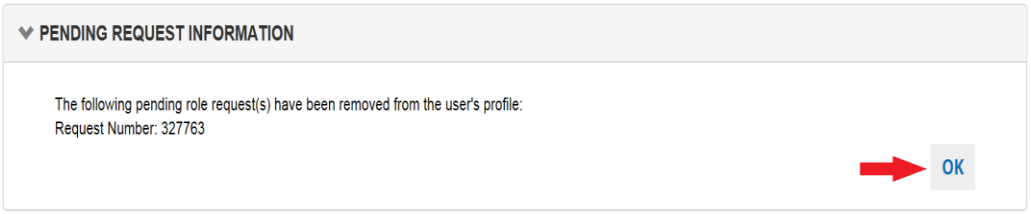
Action	
Step 3	The 'Pending Request Information' page displays. Select a pending role request related to your application and Select the **Cancel Pending Requests** button.



Step 4	Review the role requests that were selected and provide a valid justification. Select **OK**.



Step 5	A confirmation message displays. Select **OK.**



8. Updating a User's LOA

The Help Desk interface's 'Update LOA' function allows Application Help Desk Users to change a user's Level of Assurance (LOA). It is accessible through both the 'Application Search' and 'Enterprise Search'.

Important Notes

- The 'Update LOA' function is optional and configurable by application. To configure this function for your application, please follow the process outlined in "Appendix A: Requesting Configurable Help Desk Privileges".

- The criteria that determine whether an Application Help Desk User can update a user's LOA is depends on the application's established process.

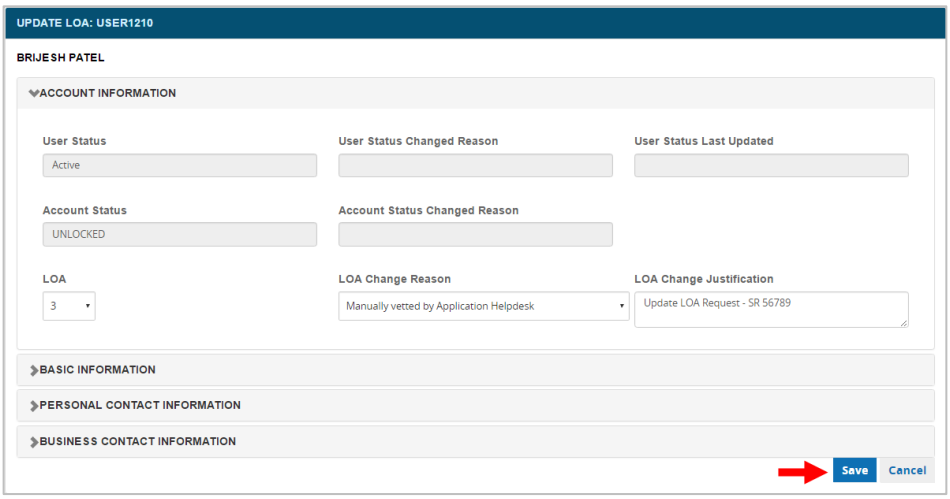
This section outlines the steps to step-up user's account LOA within the EIDM system.

	Action
Step 1	Complete the CMS-approved vetting process.
Step 2	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, perform an 'Application Search' or 'Enterprise Search', and open the 'User Details' page for the user you want to update.
Step 3	Select **Update LOA**.

Step 4 The 'Update LOA' page displays. Select a new **LOA**, select the **LOA Change Reason**, enter a **Justification**, and select **Save**.

Note

If the user's SSN field is blank, manually enter it in the field before selecting **Save**.



Step 5 A confirmation message displays. Select **OK**.

9. Unlocking an Account

The Help Desk interface's 'Unlock Account' function allows Application Help Desk Users to unlock a user's locked account. It is accessible through both the 'Application Search' and 'Enterprise Search'.

Important Note

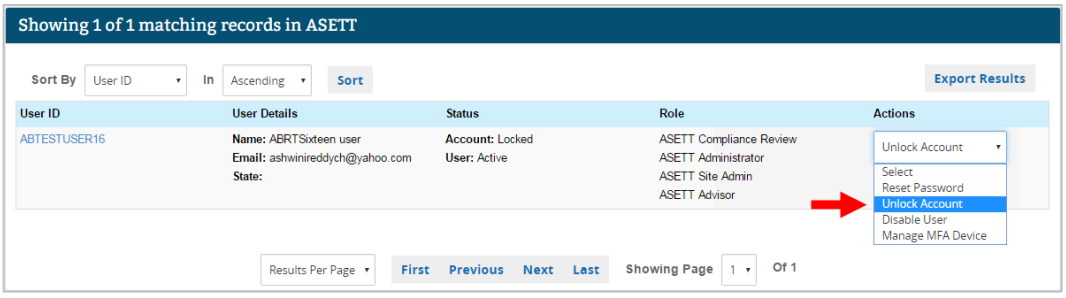
The user can also unlock their account by using the "Forgot Password" link on the CMS Enterprise Portal home page.

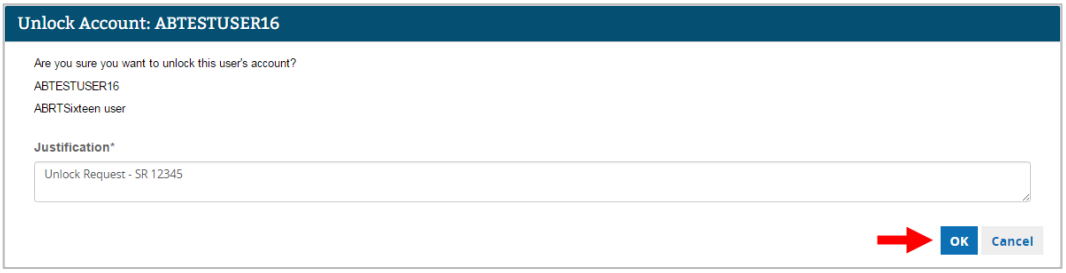
A user's account becomes locked because of any of the following circumstances:

- The user has failed three consecutive login attempts.
- The user has not logged in for a specific number of days based on the security community to which the user has been assigned (e.g., Provider Security Community is 60 days).
- An EIDM Help Desk User has locked the account manually.

This section outlines the steps to unlock a user's account within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Unlock Account** from the drop-down list in their 'Actions' column.
Step 3	The 'Unlock Account' page displays. Enter a **Justification** and select **OK**.





Action	
Step 4	A confirmation message displays. Select **OK**.

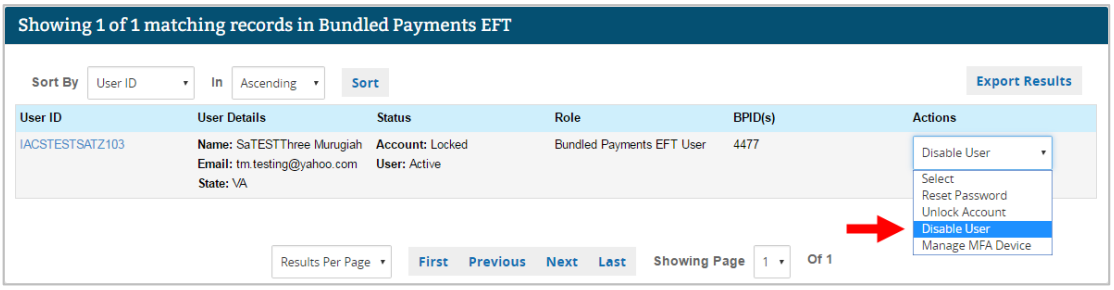
10. Disabling a User

The Help Desk interface's 'Disable User' function allows Application Help Desk Users to suspend a user's access so they can no longer log into the CMS Enterprise Portal or their applications. It is only accessible through the 'Application Search'.

Important Notes
The 'Disable User' function should only be used for security incidents.

This section outlines the steps Application Help Desk Users and EIDM Help Desk Users take to disable a user's account within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search'.
Step 2	Locate the user you wish to update and select **Disable User** from the drop-down list in their 'Actions' column.
Step 3	The 'Disable User' page displays. Enter a **Justification** and select **OK**.
Step 4	A confirmation message displays. Select **OK**.



11. Resetting a Password

The Help Desk interface's 'Reset Password' function allows Application Help Desk Users to reset a user's password so they are able to log into the CMS Enterprise Portal and their applications. It is accessible through both the 'Application Search' and 'Enterprise Search'.

Help Desk Users can perform the following actions using this function:

- E-mail Password Reset Link
- Manually Reset Password

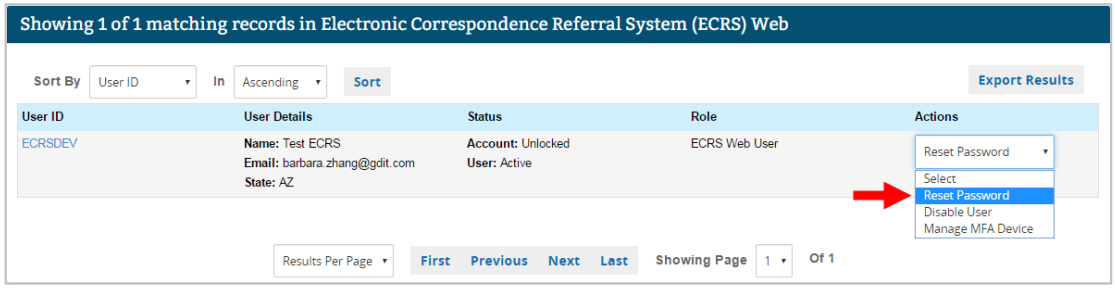
Important Notes

- The manual reset function is optional and configurable by application. To configure this function for your application, please follow the process outlined in "Appendix A: Requesting Configurable Help Desk Privileges".
- Currently, the manual password reset function is only applicable to SHIM Application Help Desk Users.
- As part of the 'Reset Password' process, the system prompts the user to change their challenge questions and answers as well.

E-mailing a Password Reset Link

This section outlines the steps Application Help Desk Users take to reset a user's password within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Reset Password** from the drop-down list in their 'Actions' column.



Action
Step 3 The 'Reset Password' page displays. Enter a **Justification** and select **OK**.

Step 4 A confirmation message displays. Select **OK**.

Note

The user's password reset link expires in 24 hours.

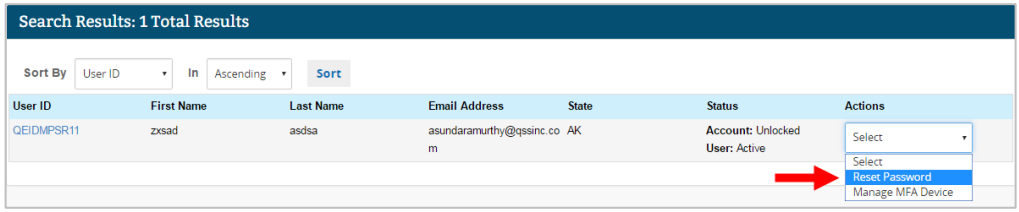
Manually Resetting a User's Password

This section outlines the steps to reset a user's password manually within the EIDM system.

Important Notes

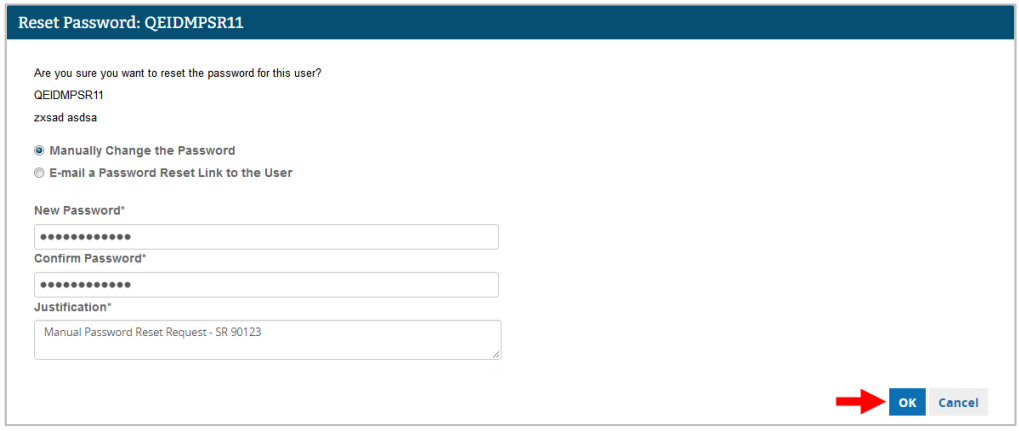
- The manual reset function is optional and configurable by application. To configure this function for your application, please follow the process outlined in "Appendix A: Requesting Configurable Help Desk Privileges".
- Currently, the manual password reset function is only applicable to SHIM Application Help Desk Users.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Reset Password** from the drop-down list in their 'Actions' column.



Step 3	The 'Reset Password' page displays. Select the **Manually Change the Password** radio button.

Step 4	Enter a **New Password**, enter the same password in **Confirm Password**, enter a **Justification**, and select **OK**.



Action	
Step 5	A confirmation message displays. Select **OK**.

12. Managing a User's MFA Devices

The Help Desk interface's 'Manage MFA Device' function allows Application Help Desk Users to view and manage a user's registered Multi-Factor Authorization (MFA) device(s). It is accessible through both the 'Application Search' and 'Enterprise Search'.

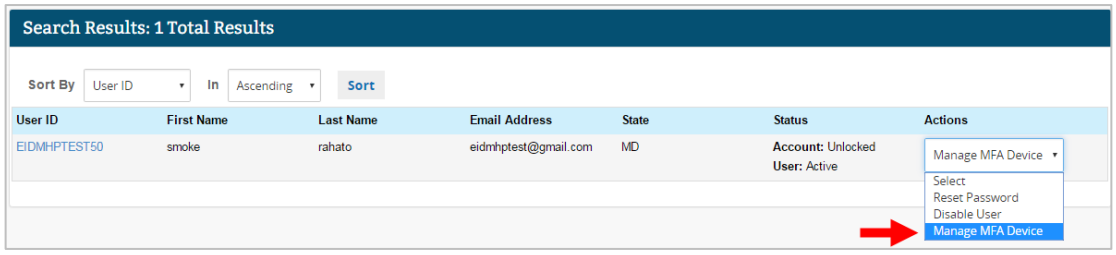
Help Desk Users can perform the following actions using this function:

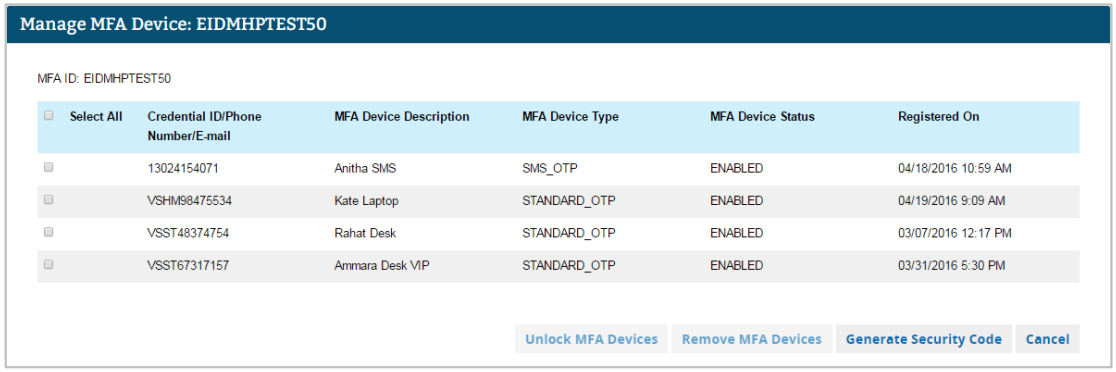
- View MFA Device(s)
- Unlock MFA Device(s)
- Remove MFA Device(s)
- Generate a Security Code

Viewing MFA Devices

This section outlines the steps to view a user's registered MFA device(s) within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Manage MFA Device** from the drop-down list in their 'Actions' column.
Step 3	The 'Manage MFA Device' page displays.

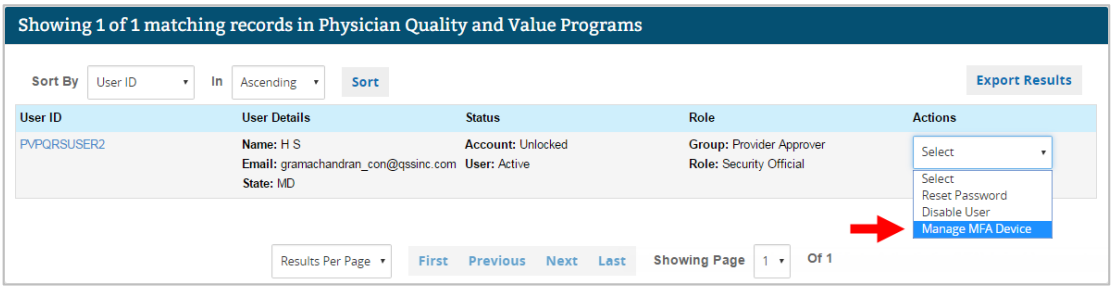




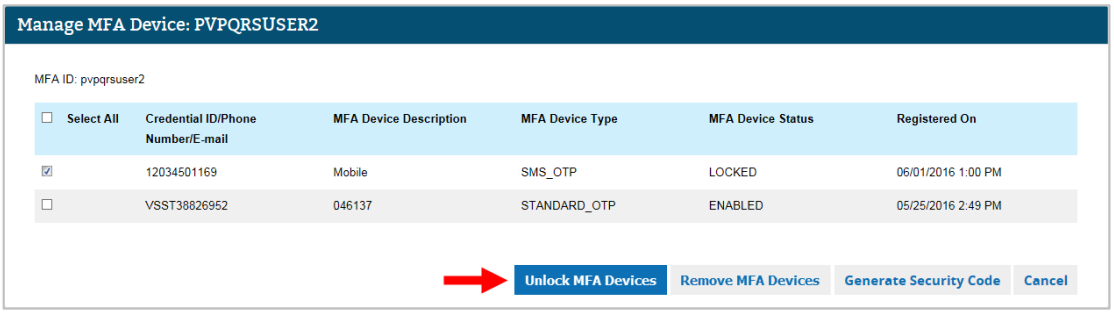
Unlocking an MFA Device

This section outlines the steps to unlock a user's registered MFA device within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Manage MFA Device** from the drop-down list in their 'Actions' column.



Step 3	The 'Manage MFA Device' page displays. Check the box for the locked device and select **Unlock MFA Devices**.



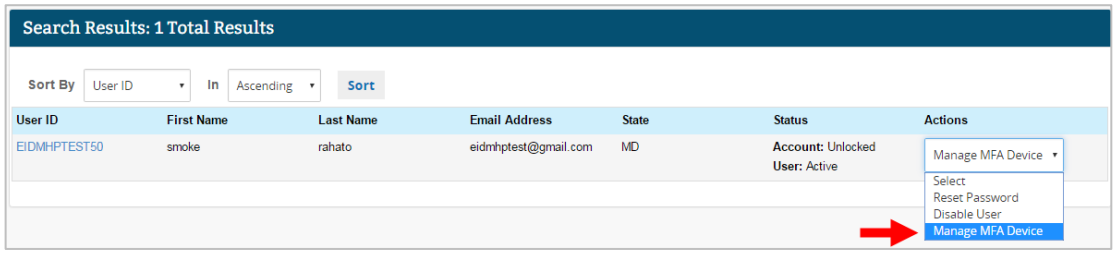
Step 4	The 'Unlock MFA Device' page displays. Select **OK**.

Step 5	A confirmation message displays. Select **OK**.

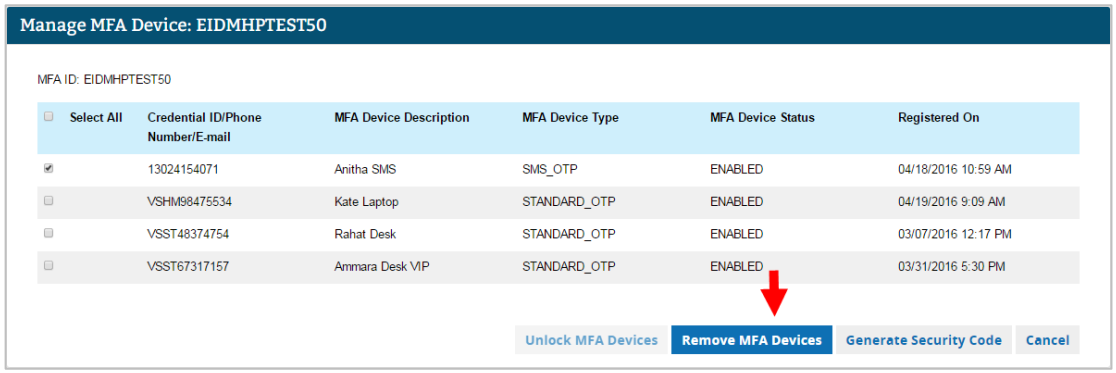
Removing an MFA Device

This section outlines the steps to remove a user's registered MFA device within the EIDM system.

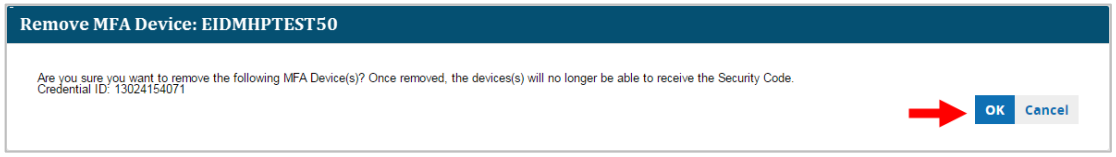
	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Manage MFA Device** from the drop-down list in their 'Actions' column.



Step 3	The 'Manage MFA Device' page displays. Check the box for the device and select **Remove MFA Device**.



Step 4	The 'Remove MFA Device' page displays. Select **OK**.

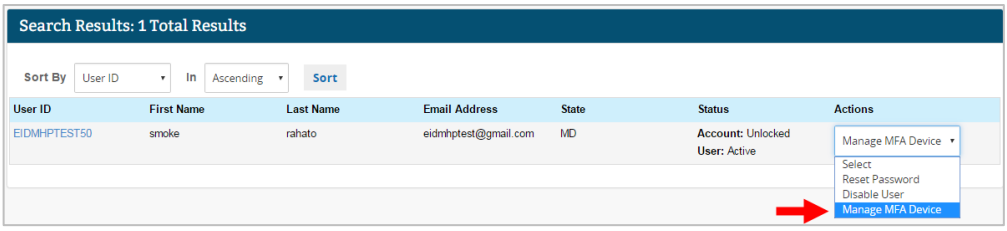


Step 5	A confirmation message displays. Select **OK**.

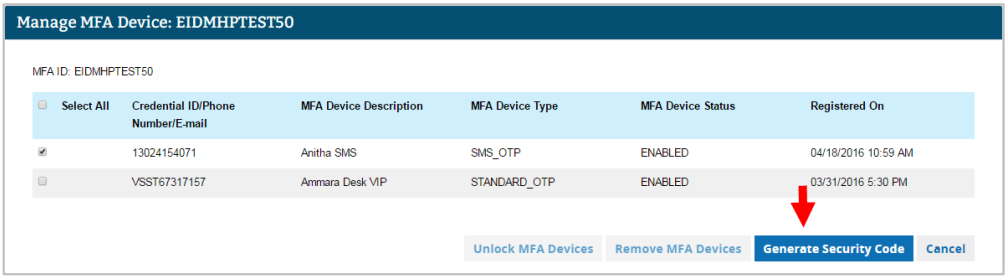
Generating a Security Code

This section outlines the steps to generate a one-time security code for the user's registered MFA device within the EIDM.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Manage MFA Device** from the drop-down list in their 'Actions' column.



Step 3	The 'Manage MFA Device' page displays. Select **Generate Security Code**.



Step 4	The 'Generate Security Code' page displays. Select a **Justification** and select **OK**.

Step 5	A confirmation message displays. If the user cannot retrieve the code via e-mail, share it with them over the phone and check the '**Security Code Provided to User by Phone**' box. Select **OK**.

13. Removing a User's Roles/Attributes

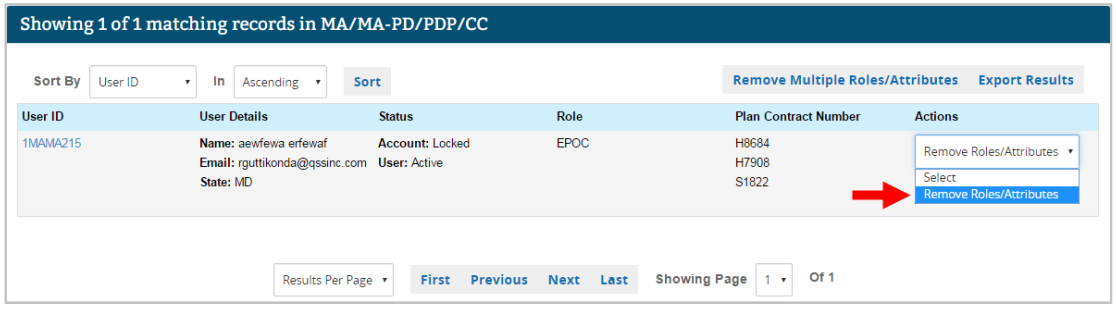
The Help Desk interface's 'Remove Roles/Attributes' function allows Application Help Desk Users to remove one or more roles or attributes from a single user's profile. It is only accessible through the 'Application Search'.

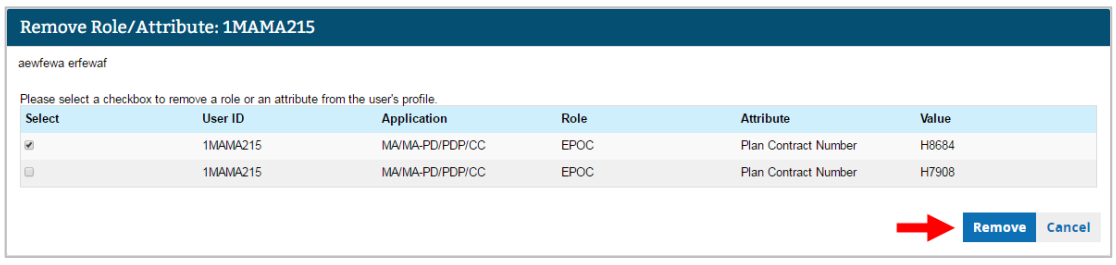
Important Notes

- The 'Remove Roles/Attributes' function is optional and configurable by application. To configure this function for your application, please follow the process outlined in "Appendix A: Requesting Configurable Help Desk Privileges".
- Application Help Desk Users must select a role in the search criteria for the 'Remove Roles/Attributes' function to be available.

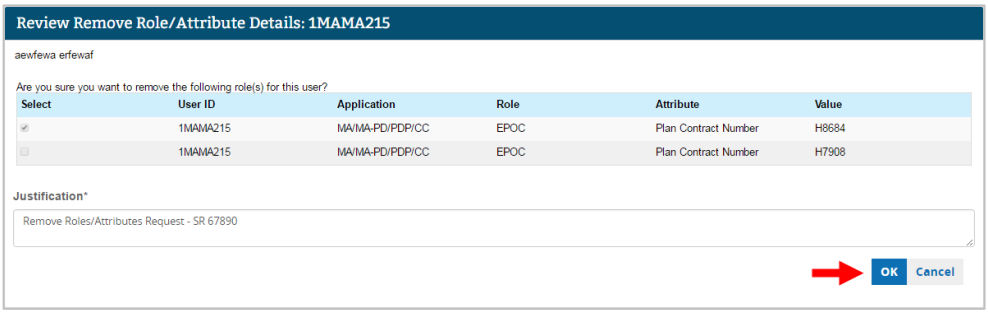
This section outlines the steps to remove one or multiple roles/attributes from a user's profile within the EIDM system.

	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and perform an 'Application Search' or 'Enterprise Search'.
Step 2	Locate the user you wish to update and select **Remove Roles/Attributes** from the drop-down list in their 'Actions' column.
Step 3	The 'Remove Roles/Attributes' page displays. Check the boxes for the roles/attributes you want to remove and select **Remove**.





Action	
Step 4	The 'Review Details' page displays. Enter a **Justification** and select **OK**.



Step 5	A confirmation message displays. Select **OK**.

14. Promoting a User

The Help Desk interface's 'Promote User' function allows Application Help Desk Users to promote the user to a higher role within an organization (e.g., Backup Security Official to Security Official). It is only accessible through the 'Application Search'.

Important Notes

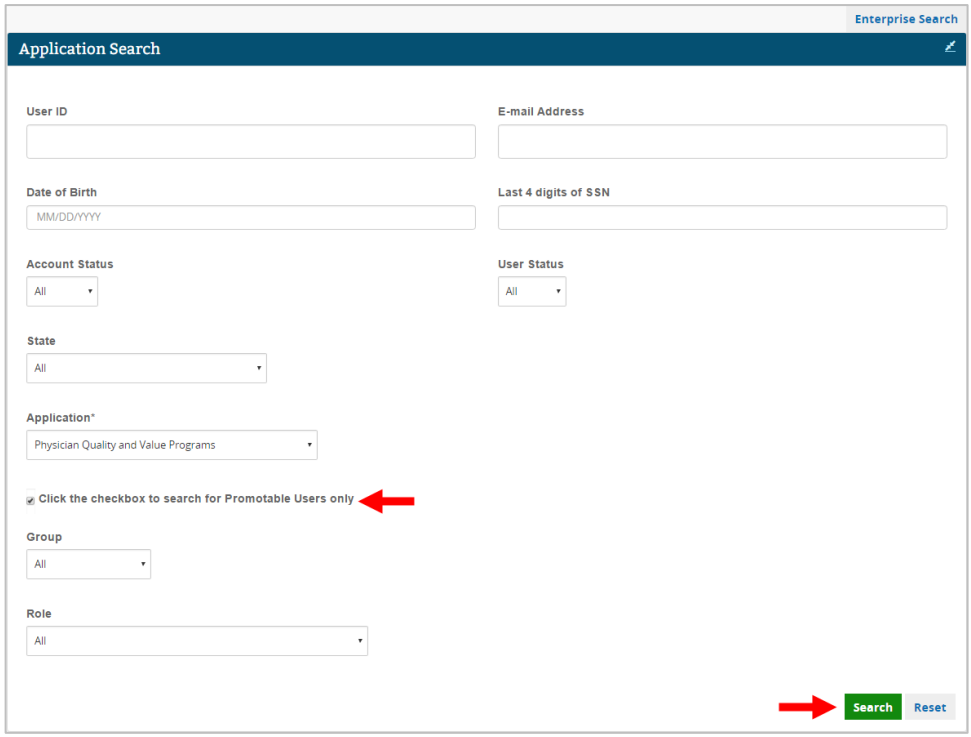
- The 'Promote User' function is optional and configurable by application if that application is organization-based. To configure this function for your application, please follow the process outlined in "Appendix A: Requesting Configurable Help Desk Privileges".
- Currently, the 'Promote User' function is only applicable to Connexion and PV/PQRS Application Help Desk Users.

This section outlines the steps to promote a user within the EIDM system.

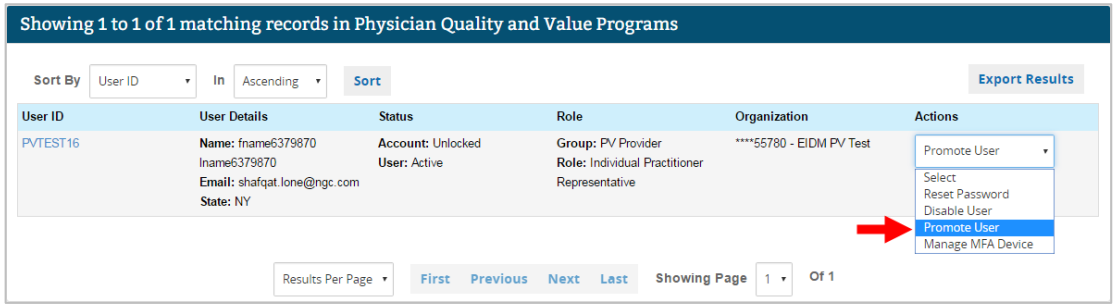
	Action
Step 1	Log into the CMS Enterprise Portal as an Application Help Desk User, access the Help Desk, and begin an 'Application Search'.
Step 2	Select an **Application**, check the '**Check this box to search for users who can be promoted**' box, and select **Search**.

Note

The checkbox displays after selecting an application configured with this function.



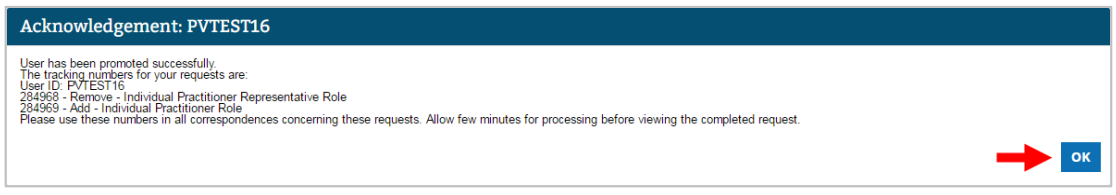
Action	
Step 3	Locate the user you wish to update and select **Promote User** from the drop-down list in their 'Actions' column.



Step 4	The 'Promote User' page display. Select the role to which you want to promote the user and select **Promote**.

Step 5	The 'Review Details' page displays. Enter a **Justification** and select **OK**.

Step 5	A confirmation message displays. Select **OK**.



15. Appendices

Appendix A: Requesting Configurable Help Desk Privileges

This section outlines the steps application Business Owners/Representatives take to request configurable Help Desk privileges in the EIDM system.

	Action
Step 1	Define the following details for each Help Desk privilege you want to request *(refer to Table 1: Help Desk Privileges for a list of privileges that can be configured)*: • **Application**: Click here to enter text. • **Role(s) to Update**: Click here to enter text. • **Help Desk Privilege**: Click here to enter text. • **Justification** (i.e., why you need this privilege): Click here to enter text.
Step 2	Use the following link to access the CMS EIDM SharePoint site and locate both the Service Request (SR) form and directions for how to submit the form: https://share.cms.gov/office/ois/Projects/ESS-PROGRAM/EIDM/SitePages/Home.aspx
Step 3	Complete the SR form with your request details defined in Step 1.
Step 4	Follow the process to submit your SR to CMS for approval.

Appendix B: Application Help Desk Information

Application *(Help Desk Name)*	Phone	E-mail
Agents and Brokers (FFM - A/B) *(XOSC)*	855-267-1515	cms_feps@cms.hhs.gov
ASETT *(ASETT Help Desk)*	703-951-6810	asett@actionet.com
BCRS *(COB&R Help Desk)*	888-268-6495	cobrhelp@strategichs.com
Bundled Payments EFT *(Bundled Payments Help Desk)*	N/A	BundledPayments@cms.hhs.gov
CERRS *(Cognosante Help Desk)*	703-206-6199	servicedesk@cognosante.com
Cisco WebEx SaaS *(WebEx Support)*	410-786-3090 *(Option 1)*	OTS_WebEx@cms.hhs.gov
COB *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
Connexion *(CBIC Help Desk)*	877-577-5331	CBIC.admin@palmettogba.com
CPMS *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov
CSR *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
DBidS/ DMEPOS *(CBIC Help Desk)*	877-577-5331	CBIC.admin@palmettogba.com
ECRS *(EDI Help Desk)*	646-458-6740	ECRSHelp@EHMedicare.com
ELMO *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
EPPE *(EPPE Help Desk)*	844-377-3382	eppe@cms.hhs.gov
e-RPT *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
ESD *(ESD Application Support)*	TBD	TBD
FCSO aka The Spot *(FCSO Help Desk)*	855-416-4199	FCSOSpotHelp@FCSO.com

Application *(Help Desk Name)*	Phone	E-mail
FFSDCS *(ASP Help Desk)*	844-876-0765	aspHelpDesk@dcca.com CLFShelpdesk@dcca.com
Gentran *(Gentran Support)*	N/A	Gentran-support@cms.hhs.gov
HDT *(MCARE/HDT Help Desk)*	866-324-7315	mcare@cms.hhs.gov
HIOS *(XOSC)*	855-267-1515	cms_feps@cms.hhs.gov
IC (Innovation Center) *(IBOSC and IC Help Desks)*	844-711-CMMI *(Option #1)* 844-280-5628 800-381-4724	cjrsupport@cms.hhs.gov HHVBPquestions@cms.hhs.gov cpcplus@telligen.com
ISV *(ISV Help Desk)*	N/A	ISV-Support@cms.hhs.gov
MACPro *(MACPro Help Desk)*	301-547-4688	MACPro_HelpDesk@cms.hhs.gov
MARx *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
MCU *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov
MDR *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
MED *(EUS Help Desk)*	866-484-8049	eussupport@cgi.com
MLMS *(MLMS Help Desk)*	N/A	MLMSHelp Desk@cms.hhs.gov
MyCGS *(MyCGS Help Desk)*	866-270-4909	cgs.dme.mac.email.inquiries@cgsadmin.com
Novitas *(Novitas Help Desk)*	855-880-8424	WebsiteEDI@novitas-solutions.com
Open Payments *(Open Payments Help Desk)*	855-326-8366	OpenPayments@cms.hhs.gov
Physicians Value aka PV *(PV Help Desk)*	888-734-6433	pvHelp Desk@cms.hhs.gov
PMDA *(PMDA Help Desk)*	443-775-3226	pmda1115_cvp_help@cvpcorp.com

Application *(Help Desk Name)*	Phone	E-mail
PQRS *(QualityNet Help Desk)*	866-288-8912	qnet-hd-support-queue@hcqis.org
PS&R/STAR *(EUS Help Desk)*	866-484-8049	eussupport@cgi.com
QARM *(ESRD Help Desk)*	866-288-8912	QNETSupport-ESRD@hcqis.org
QMAT *(CEC Help Desk)*	888-734-6433	ESRD-CMMI@cms.hhs.gov
Salesforce *(CMS Salesforce and Force.com Information Center)*	888-734-6433 *(Option 5)*	CMMIForceSupport@cms.hhs.gov
SERTS *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov
SERVIS *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov
SHOP/SHIM *(SHOP Call Center/Support)*	800-706-7893	N/A
SLS *(SLS Support)*	N/A	sls@navahq.com
T-MSIS *(T-MSIS Help Desk)*	N/A	T-MSIS_HelpDesk@cms.hhs.gov
UCM *(UCM Help Desk)*	844-826-3375	ucmsupport@cms.hhs.gov
VMS Client Letter *(GDIT Technical Help Desk)*	443-275-6946 *(Option 2)*	THD@gdit.com
zONE *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov

Table 3: Application Help Desks

Appendix C: Important Terms

Term	Definition
Application Approver	users who approve End User role requests *Note: In some applications, Application Help Desk Users act as Approvers who are responsible for approving End User and/or Approver role requests.*
Application Help Desk User	an EIDM system user type that provides Tier 1 Help Desk support for End Users
Application Search	a type of search that allows Help Desk Users and Approvers to search and manage accounts for users with a role in their application
Authorizer	an EIDM system user type that is responsible for approving Approver or Help Desk User role requests
Disabled	a user status that indicates the user can no longer log into the CMS Enterprise Portal or their applications
EIDM Help Desk User	an EIDM system user type that provides Tier 2 Help Desk support for all EIDM-integrated application users
End User	an EIDM system user type that registers with EIDM for access to CMS applications
Enterprise Search	a type of search that allows Application Help Desk Users to search and manage accounts for users who do not have a role (e.g., helping users who called the wrong Help Desk or stepping up a user who may or may not have an application role)
Help Desk User	a general term used to identify both Application Help Desk Users and EIDM Help Desk Users
Locked	an account status that indicates the user has either mistyped his/her password 3 times, has not accessed their account in a specific time period, or has entered the wrong challenge questions 3 times during profile updates
Security Community	categories used to determine the security guidelines (e.g., inactivity, password expiry, password complexity, password reuse) that the user will be subject to as a registered EIDM user 1. **Professionals**: Users acting on behalf of employers, Issuers, providers, 3rd party buyers, brokers, Accountable Care Organization (ACO), and Quality Improvement Organization (QIO) 2. **Consumers**: Users acting on behalf of self, family, or business 3. **Organizational Users**: CMS employees or contractors doing work on behalf of CMS 4. **Default**: The community to which users belong when they first register to EIDM and you can choose for the users to continue to stay in this community.

Table 4: Important Terms

Appendix D: Acronyms

Acronym	Literal Translation
ACO	Accountable Care Organization
AIA	Automated Intervention Application
AO	Authorized Official
BAO	Backup Authorized Official
BCRC	Benefits Coordination & Recovery Center
CAHPS	Consumer Assessment of Healthcare Providers and Systems
CBA	Competitive Bidding Area
CBIC	Competitive Bidding Implementation Contractor
CGS	Celerian Group Administrators, LLC (collectively "CGS")
CHIP	Children's Health Insurance Program
CLFS	Clinical Laboratory Fee Schedule
CMS	Centers for Medicare & Medicaid Services
COB	Coordination of Benefits
CPC	Comprehensive Primary Care
CSR	Customer Service Representative
CWF	Common Working File
DBidS	DMEPOS Bidding System
DCCA	Data Computer Corporation of America
DME	Durable Medical Equipment
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies
ECRS	Electronic Correspondence Referral System
EFT	Electronic File transfer
EIDM	Enterprise Identity Management
EP	Eligible Professional
EPOC	External Point of Contact (EPOC)
FCSO	First Coast Service Options (The SPOT)
FFSDCS	Fee for Service Data Collection System
GPRO	Group Practice Reporting Option
GUI	Graphical User Interface
HDT	HIPAA Eligibility Transaction System (HETS) Desktop
HETS	HIPAA Eligibility Transaction System

Acronym	Literal Translation
IDP	Identity Proofing
IVR	Interactive Voice Response
LBN	Legal Business Name
LOA	Level of Assurance
LSA	Local System Administrator
MA	Medicare Advantage
MAC	Medicare Administrative Contractor
MAPD	Medicare Advantage - Prescription Drug
MARx	Medicare Advantage and Prescription Drug System
MCO	Medicaid Managed Care Organization
MDR	Medicaid Drug Rebate
MED	Medicare Exclusion Database
MFA	Multi-Factor Authentication
MMP	Medicare and Medicaid Plan
MSP	Medicare Secondary Payer
NPI	National Provider Identifier
OOW	Out-of-Wallet
OTP	One-time Password
PDE	Prescription Drug Event
PDP	Prescription drug Plan
POS	Point Of Service
POS	Point of Sale
POSFE	Point-of-Sale Facilitated Enrollment
PQIP	Physician Quality Initiatives Portal
PQRS	Physician Quality Reporting System
PS&R	Provider Statistical and Reimbursement
PTAN	Provider Transaction Access Number
PV	Physician Value
PY	Payment Year
QRUR	Quality and Resource Use Report
RACF	Resource Access Control Facility
RAPS	Risk Adjustment Processing System

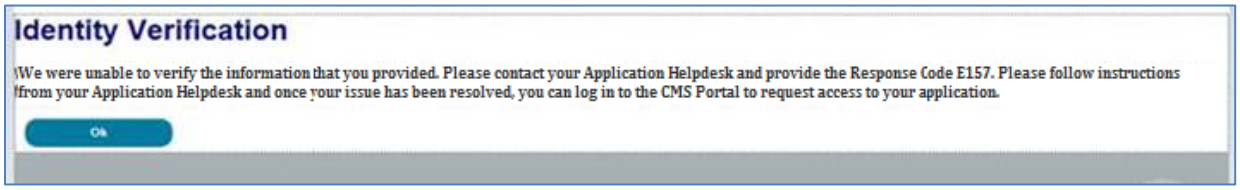
Acronym	Literal Translation
RIDP	Remote Identity Proofing
SHIP	State Health Insurance Plans
SMS	Short Message Service
SPAP	State Pharmacy Assistance Programs
SR	Service Request
SSN	Social Security Number
STAR	System for Tracking Audit and Reimbursement
TIN	Taxpayer Identification Number
TT	Trouble Ticket
UI	User Interface
VMS	ViPS Medicare System
XLC	eXpedited Life Cycle
XLS	Microsoft Excel Workbook

Table 5: Acronyms

Appendix E: Experian Identity Proofing Error Codes

This section outlines the different types of errors that can arise during the identity proofing process during EIDM Account Step-up. Each error code corresponds to a specific system issue, and identifies whether the issue is taking place within EIDM or Experian. This will assist Help Desk representatives in identifying where the user's issue is taking place, allowing for more accurate escalation of the error.

The Experian error codes are displayed to the end user at the time of failing identify proofing after contacting Experian Verification Support Services. The end user can provide the error code displayed in the message box to the Application Help Desk representative to assist with the next steps in completing identity proofing.



Error Code	Comments	Next Steps
E106	Web service call failure	E106 indicates there was technical error during the ID verification process and the user has to retry ID verification after some time.
E150	Consumer is minor	Suggested Approach for Help Desk: 1. E150 indicates the user undergoing ID proofing is a minor as per Experian records. The user will not be phone proofed by the Experian Call center. 2. The Help Desk will have to manually ID proof the users if the users are eligible for the specific role in the application by verifying their documents.
E151	Information on the inquiry indicates a fraud alert on the consumers credit file	Suggested Approach for Help Desk: 1. Experian records indicate there is a fraud alert/victim statement on the user's credit file and the user cannot be verified by the Experian Phone center. 2. The Application Help Desk will have to manually ID proof the user by verifying the user's legal documents.
E152	SSN required to access consumer's file	Suggested Approach for Help Desk: 1. Experian was not able to uniquely identify the user based on the information provided and SSN is required to find the user. 2. The Application Help Desk may ask the user to try RIDP remotely by providing SSN. 3. Alternative approach for the Help Desk is to manually ID proof the users by verifying the legal documents.

<table>
<tr><th>Error Code</th><th>Comments</th><th>Next Steps</th></tr>
<tr><td>E153</td><td>Unable to standardize current address. The address the consumer provided could not be processed by USPS as a valid residential address.</td><td>Suggested Approach for Help Desk:
1. Experian records indicate the address provided was a business address and not a residential address.
2. The Application Help Desk may ask the user to verify their address and try RIDP remotely with their residential address.
3. The Alternative approach for the Help Desk is to manually ID proof the users by verifying their legal documents.</td></tr>
<tr><td>E154</td><td>User had a frozen credit card file</td><td>Users will have to call the Experian Phone center.</td></tr>
<tr><td>E155</td><td>Invalid surname or less than two characters in length</td><td>Suggested Approach for Help Desk:
1. Notify the consumer that surnames must be at least two characters. If consumer’s surname is less than 2 characters they must be manually ID proofed.
2. The Application Help Desk may ask the user to verify their last name and try RIDP remotely with the updated last name.
3. If the user’s last name is less than 2 characters, the Help Desk may have to manually ID proof them by verifying the legal documents.</td></tr>
<tr><td>E156</td><td>Current Address exceeds maximum length</td><td>Suggested Approach for Help Desk:
1. The inputted address exceeded the maximum length.
2. The Application Help Desk may ask the user to verify their address length as per the below table and try RIDP remotely with the updated address.
3. The table below describes the address length accepted by Experian.
<table>
<tr><th>Tag</th><th>Max length</th><th>Description</th></tr>
<tr><td>Current Address</td><td>N/A</td><td>Start tag for Primary Applicant Current Address elements (CA-)
Entire address cannot exceed 118 characters (Street + City + State + Zip)</td></tr>
<tr><td>Street</td><td>60</td><td>Street address, PO Box, Route Number</td></tr>
<tr><td>City</td><td>38</td><td>City name</td></tr>
<tr><td>State</td><td>2</td><td>State name</td></tr>
<tr><td>Zip</td><td>10</td><td>ZIP code</td></tr>
</table>
4. If the user’s address exceeds the address length specified above, the Help Desk may have to manually ID proof them by verifying the legal documents.</td></tr>
</table>

Error Code	Comments	Next Steps
E157	Experian records indicate the user is deceased	Suggested Approach for Help Desk: 1. E157 indicate the user is reported as deceased as per Experian Records. 2. The Application Help Desk may ask the user to call SSA and verify their records with them. 3. Once the SSA records are updated the user can try ID proofing again. *(Note: This approach might take several days/months.)* 4. The Alternative approach for Help Desk is to manually ID proof the users by verifying their legal documents.
E158	Input validation error	Suggested Approach for Help Desk: 1. The inputted data did not meet Experian's validation rules. Recommend that the user verify their information and try again. 2. The Application Help Desk will have to manually ID proof the users by verifying their legal documents.
E159	Session Timeout: This occurs when the user takes longer than 10 minutes to respond to the Out of Wallet questions	Suggested Approach for Help Desk: 1. Experian records indicate user failed to answer the Experian ID Verification questions in 10 minutes and hence they were not able to successfully complete the ID verification process. 2. The Help Desk may ask the users to retry ID verification with the system by being ready with their personal and financial questions and answer the questions within 10 minutes. 3. The Alternative approach for the Help Desk is to manually ID proof the users by verifying their legal documents.
E160	Internal Experian Error codes	E160 indicates there was technical error during the ID verification process and the user has to retry ID verification after some time.
E161	Other Precise ID system error	Suggested Approach for Help Desk: 1. Experian records indicate address provided by the user may not be updated as the recent address in USPS. 2. The Help Desk may ask the users to retry ID verification by providing an old residential address. 3. The Alternative approach for the Help Desk is to manually ID proof the users by verifying their legal documents.
E162	Exception case	Users will have to call the Experian Phone center.
E163	User was not found	Users will have to call the Experian Phone center.
E239	User has exceeded maximum ID proofing attempts	Users will have to call the Experian Phone center.

Table 6: Experian IDP Error Codes