CENTERS FOR MEDICARE & MEDICAID SERVICES

CMS **Enterprise Identity Management (EIDM)**

User Guide for Approvers

Working Copy Version 0.1 Release 14 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.

Issued: June 2016

This page is intentionally blank.

Table of Contents

1. Introduction 1
   - What is EIDM? 1
   - What is the EIDM User Guide for Approvers? 1
2. Before You Begin 2
   - Verify Your Computer Settings 2
   - What you may need before you begin 3
   - Logging into the CMS Enterprise Portal 4
3. Approval 8
   - How the approval process works (quick overview) 8
   - Using the Pending Approvals Feature 10
   - Pending Approvals 17
4. Annual Certification 25
   - Certifying Manually Approved Roles 26
   - Using the 'Search Users' Feature 34
   - Validated Roles 41
   - Account Review 43
5. Manage Users 45
   - How to search for a user 45
   - How to remove a role attribute 50
   - How to remove a role 56
   - How to remove multiple roles or attributes 62
   - How to use the Export Results feature 68
6. Help Desk Information 72
   - Application Help Desks 72
7. Approver Roles and Functions 75
8. Acronyms 76

EIDM User Guide for Approvers

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) system 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 User Guide for Approvers?

The EIDM Guide for Approvers is for individuals who have Approver authority. This guide provides basic step-by-step instructions on how to approve and manage users.

2. Before You Begin

The following steps are recommended to optimize computer settings and ensure proper access to the CMS system:

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:
You should 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 versions 8-11, Firefox, Google Chrome, and Safari.

Verify Your Computer Settings

This section outlines the steps to verify your computer settings.

	Action
Step 1	Verify your screen resolution. **Windows XP:** Select the **Start** button, select **Control Panel**, and select **Display**. You will see a horizontal **Resolution** slider with your current setting below it. **Windows Vista:** Select the **Start** button, select **Control Panel**, find **Appearance and Personalization**, and select **Display Settings**. Ensure the correct monitor is currently selected. Note your settings below the horizontal **Resolution** slider and select **Cancel** to leave your settings as they are. **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 8: Open your browser, select the **Tools** button, point to **Pop-up Blocker**, and select **Turn Off Pop-up blocker**.
Internet Explorer 9, 10, and 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.

What you may need before you begin

Prior to requesting access, you should have received instructions from your organization or CMS contact. The instructions should include application specific information you may need to complete the request, such as:

- Social Security Number (SSN)/Taxpayer Identification Number (TIN)
- Legal Business Name (LBN) or Organization
- Application Name
- Application Role
- Other information specific to your application, for example, Contract Number, Gentran Mailbox, National Provider Identifier (NPI), Organization number.
- You will have to create a User ID and password of your choosing if you do not already have a User ID and password. EIDM allows you to create a User ID up to 74 characters; however, some applications have restrictions on the number of

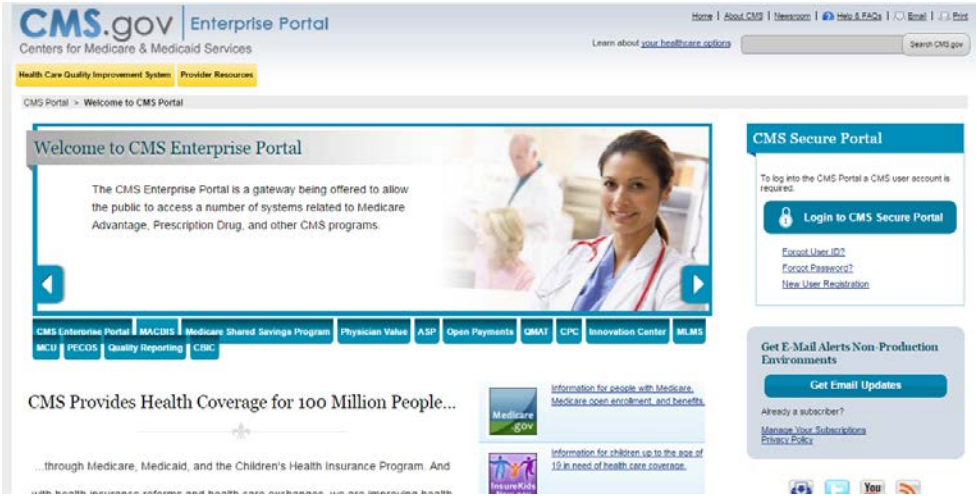
characters, and special characters, you can have in the User ID you create. Check with your CMS point of contact to identify restrictions for your application.

- Not every CMS application requires the same information, so it is important to get the specifics directly from your organization or CMS contact.

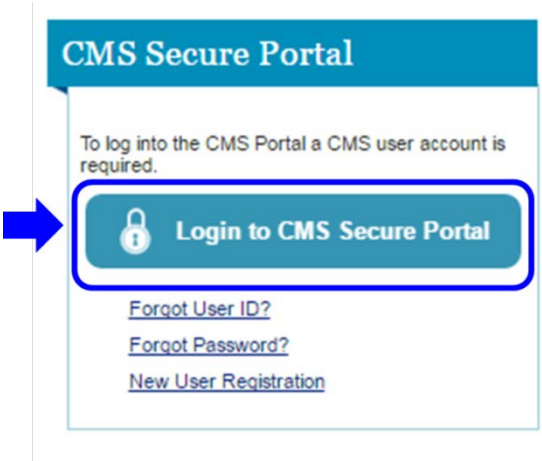
Logging into the CMS Enterprise Portal

This section provides information on how to Login using your user name and password. The following are the basic step-by-step instructions.
If you do not have an EIDM User name and password or a role please refer to the **CMS EIDM User Guide** for details on how to register in EIDM to create your User ID and request a role.

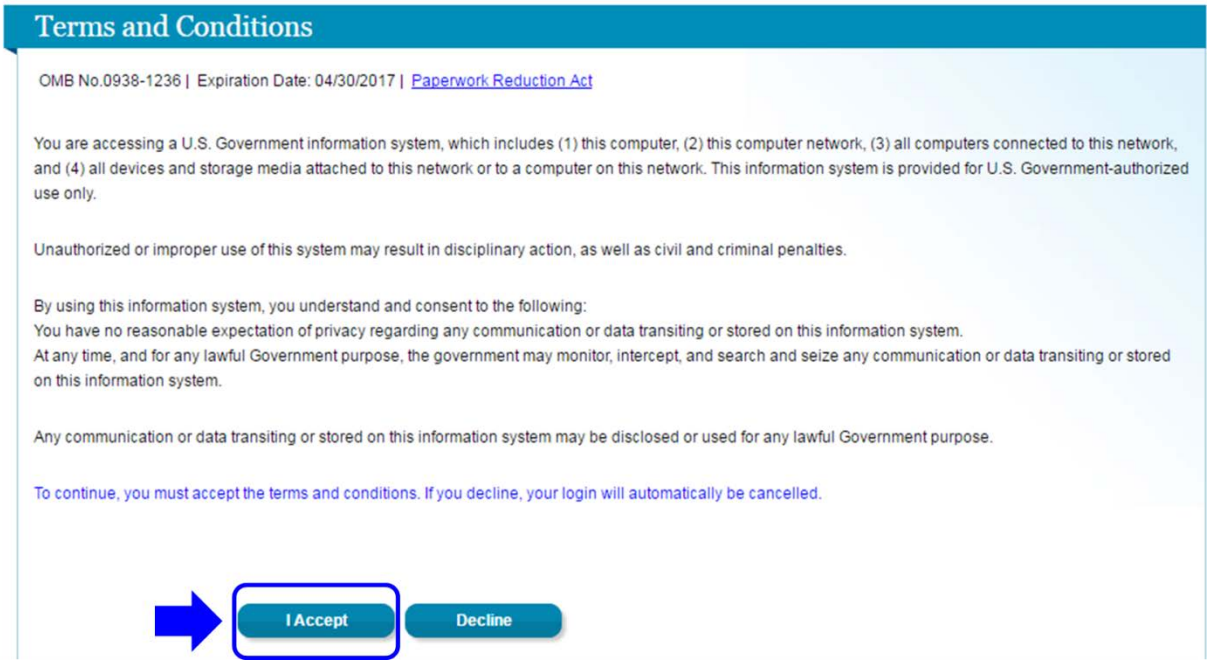
	Action
Step 1	Navigate to https://portal.cms.gov. The **CMS Enterprise Portal** page is displayed, as illustrated below.



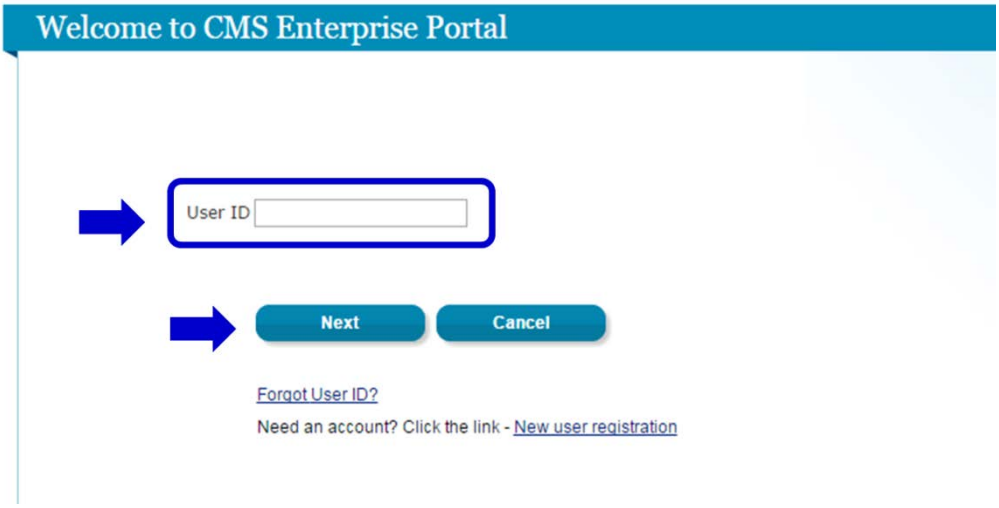
Step 2	Select **Login to CMS Secure Portal**.



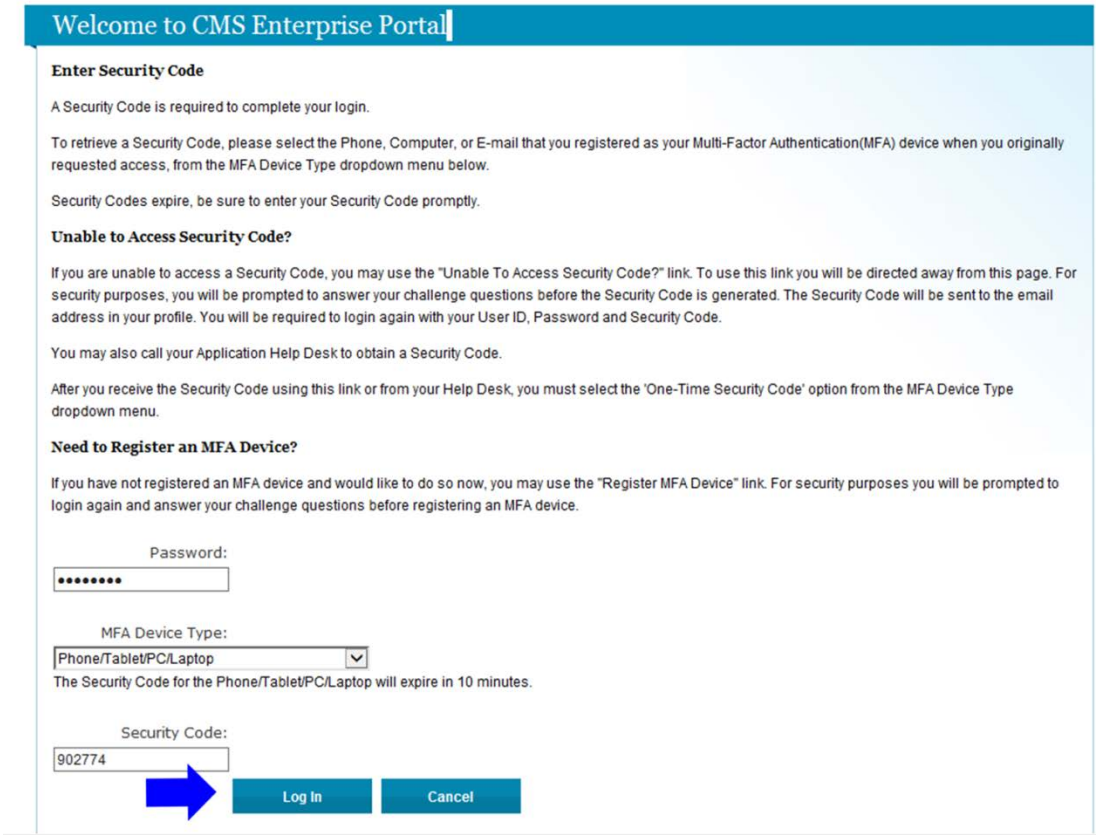
Action	
Step 3	Read the **Terms and Conditions** and select **I Accept** to continue.



Step 4 Enter your User ID and select **Next** to continue.



Action	
Step 5	Enter your Password, MFA Device Type, and Security Code. Select **Log In**.

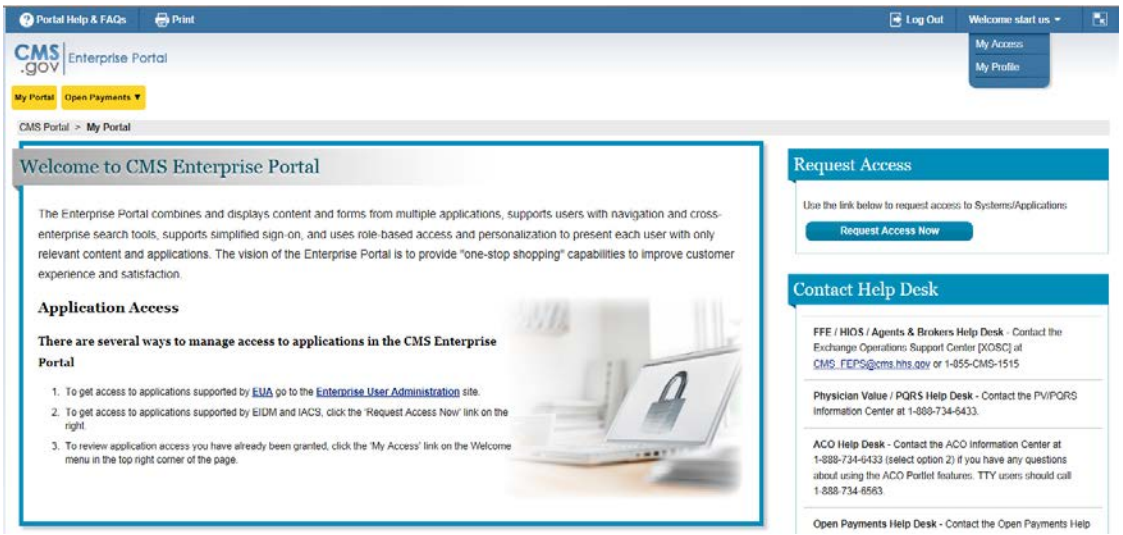


Note:

For more information on Multi-Factor Authentication (MFA) please refer to the **CMS EIDM User Guide**.

After logging in, the **Welcome to CMS Enterprise Portal** page is displayed.

Action


Portal Help & FAQs
Print
Log Out
Welcome start us
My Access
My Profile
CMS .gov Enterprise Portal
My Portal
Open Payments
CMS Portal > My Portal
Welcome to CMS Enterprise Portal
The Enterprise Portal combines and displays content and forms from multiple applications, supports users with navigation and cross-enterprise search tools, supports simplified sign-on, and uses role-based access and personalization to present each user with only relevant content and applications. The vision of the Enterprise Portal is to provide "one-stop shopping" capabilities to improve customer experience and satisfaction.
Application Access
There are several ways to manage access to applications in the CMS Enterprise Portal
1. To get access to applications supported by EUA go to the Enterprise User Administration site.
2. To get access to applications supported by EIDM and IACS, click the 'Request Access Now' link on the right.
3. To review application access you have already been granted, click the 'My Access' link on the Welcome menu in the top right corner of the page.
Request Access
Use the link below to request access to Systems/Applications
Request Access Now
Contact Help Desk
FFE / HIOS / Agents & Brokers Help Desk - Contact the Exchange Operations Support Center [XOSC] at CMS_FEPS@cms.hhs.gov or 1-855-CMS-1515
Physician Value / PQRS Help Desk - Contact the PV/PQRS Information Center at 1-888-734-6433.
ACO Help Desk - Contact the ACO Information Center at 1-888-734-6433 (select option 2) if you have any questions about using the ACO Portlet features. TTY users should call 1-888-734-6563.
Open Payments Help Desk - Contact the Open Payments Help

3. Approval

This section provides information on how the approval process works, the approval structure for each application, and detailed steps on how to find, review, approve, reject or defer a pending request.

How the approval process works (quick overview)

The following is a quick overview of the key steps in the process of locating, reviewing, and approving submitted requests.

1. After a request has been submitted for approval, an E-mail notification is sent to every approver authorized to review and approve this request.
2. The request is also sent to, and listed on, the **My Pending Approvals** page for every approver, authorized to review and approve this request.
3. To reach the **My Pending Approvals** page, **navigate to** https://portal.cms.gov.
4. On the CMS Portal page, **select** the **Login in to CMS Secure Portal** link.
5. **Accept** the Terms and Conditions.
6. **Log in** with your User ID and password.

   After logging in, EIDM will check to see if you are an approver for one or more applications.
7. On the **Welcome to CMS Enterprise Portal** page, **select** the down arrow icon that appears next to your name at the top of page. Then, **select My Access** from the drop down menu to continue.

   Alternatively, you may **select Request Access Now** to continue.
8. After the **Access Catalog, My Access** and **My Pending Requests** sections are displayed, **select Other Actions** in the **My Access** section.
9. On the View and Manage My Access page, **select My Pending Approvals**.
10. The **Pending Approvals** page is displayed.
11. By default, all of the pending approvals you are authorized to review and approve are listed on your **Pending Approvals** page. Only authorized approvers for the application can view and approve submitted requests for the application. You cannot view the pending approvals of other applications, unless you have also been approved to be an authorized approver in those applications. Authorized approvers of other applications cannot view or approve your application's pending requests.
12. The "**Search Requests**" feature may be used to search for and locate specific pending requests. For example, the Search Requests feature may be used to search for pending requests by first name, last name, partial first name, partial last name, request number, date the request was submitted, or even using the "Keywords" search option. The search results will only list pending approvals the approver is authorized to review and approve.

13. **Select** and **view** one of the pending requests.
14. After reviewing the information submitted with the request, you can **approve**, **reject**, or **defer** the request. If you approve or reject the request, you will have to provide a justification for the approval or rejection. If you defer the request, no action is taken, and the pending request will remain on the My Pending Approvals page. Pending requests will expire after 60 days unless they are approved or rejected.
15. After a pending request is **approved** or **rejected** by an approver, an E-mail notification is sent to the person that submitted the request. The E-mail will include the justification the approver submitted with the approval or rejection.

Using the Pending Approvals Feature

The following are the basic step-by-step instructions on how to use the **Pending Approvals** feature to find, review, approve, reject, or defer a pending request.

The **My Pending Approvals** link is located on the **View and Manage My Access** page and can be accessed by EIDM users that have Approval authority.

Note

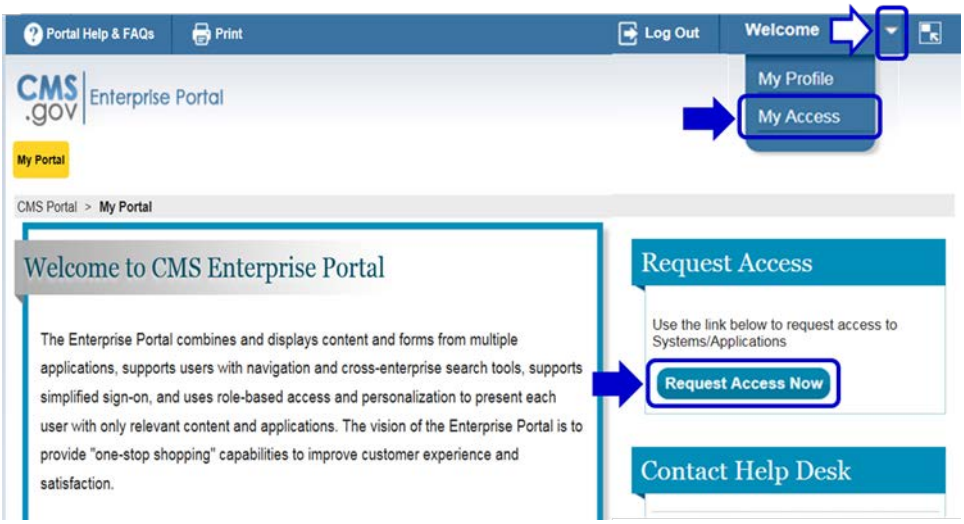
To approve a pending request for one of the applications listed below**BEGIN HERE**.

- ASETT
- ASP
- EPPE
- ESD
- IC
- DHD
- MACPro
- MCU
- MLMS
- Open Payments
- SHIM
- T-MSIS
- zONE

For all other applications, please **FOLLOW THESE STEPS**.

	Action
Step 1	After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed. Select the down arrow icon that appears next to your name at the top of page. Then, select **My Access** from the drop down menu to continue. Alternately, you may select **Request Access Now** to continue. **Note**: After logging in, EIDM will check to see if you are an approver for one or more applications.

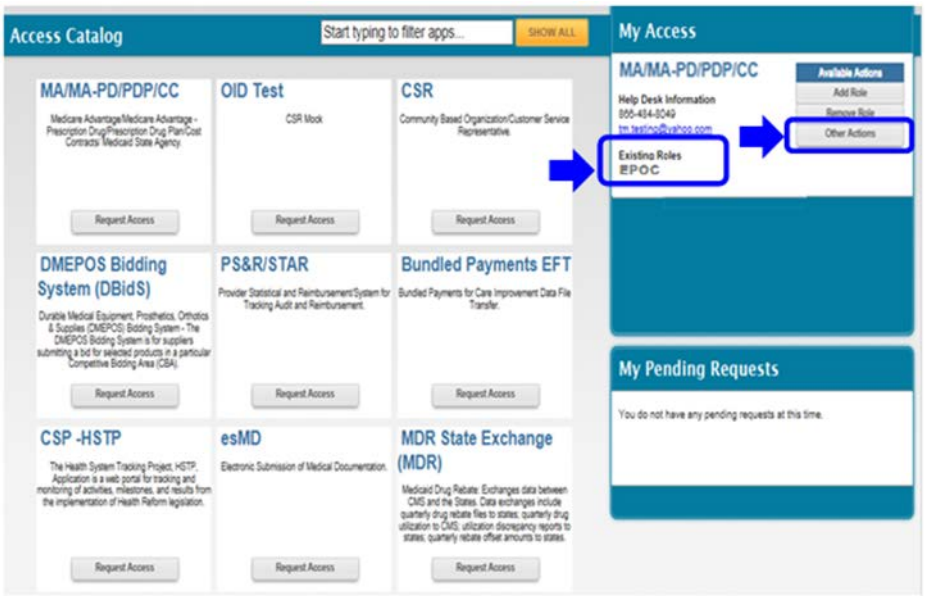
Action



Step 2 The **Access Catalog**, **My Access** and **My Pending Requests** sections are displayed.

Any existing roles you have in each application are displayed in the **My Access** section.

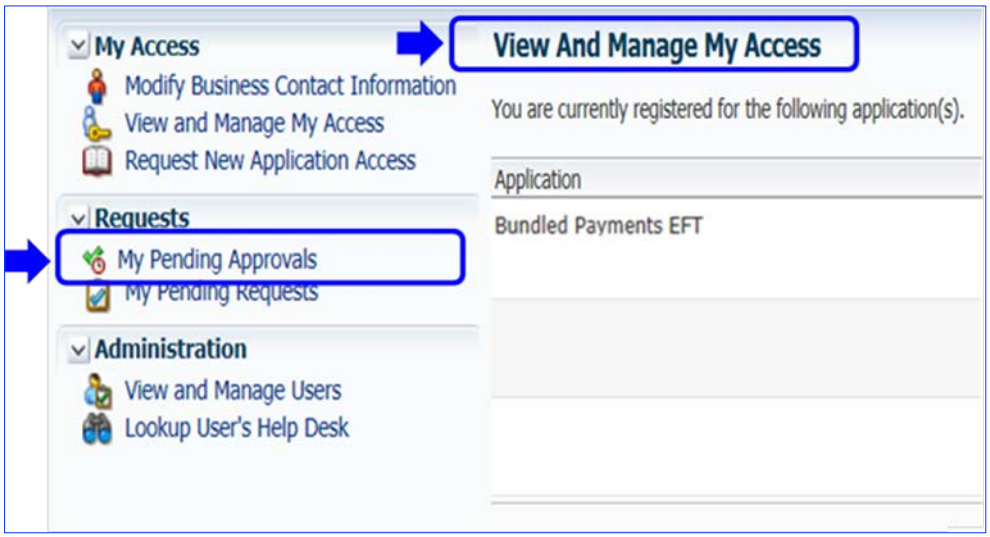
Select **Other Actions** in the **My Access** section to continue. If there are multiple **Other Actions** options displayed, you may select <u>any</u> "Other Actions" option to continue.



Step 3 The **View and Manage My Access** page is displayed.

Select **My Pending Approvals** to continue.

Action

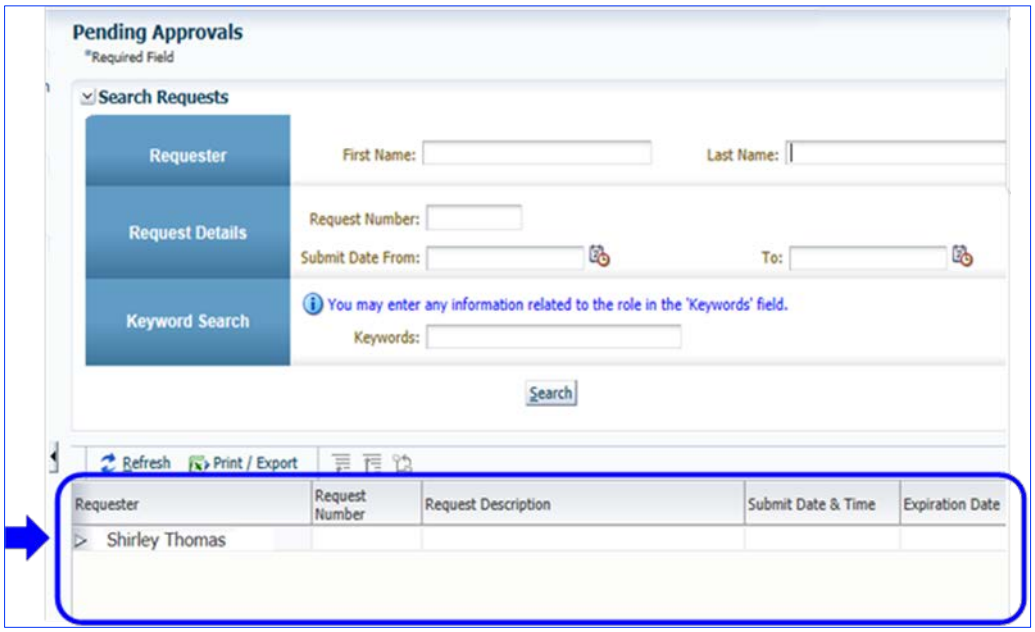


Step 4 The **Pending Approvals** page is displayed.

By default, all of the pending approvals you are authorized to review and approve are listed.

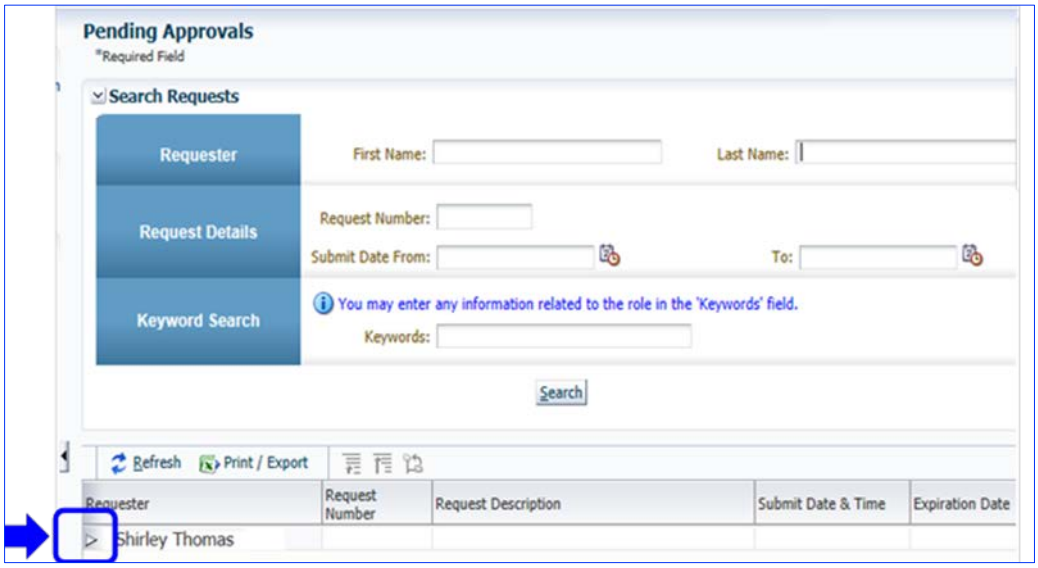
You may also use the **Search Requests** features to narrow your search. Search instructions and tips are provided on the **Pending Approvals** page.

In the example below, we only have one pending request for approval.



Step 5 To view the pending request, first select the single right arrow icon that appears before the

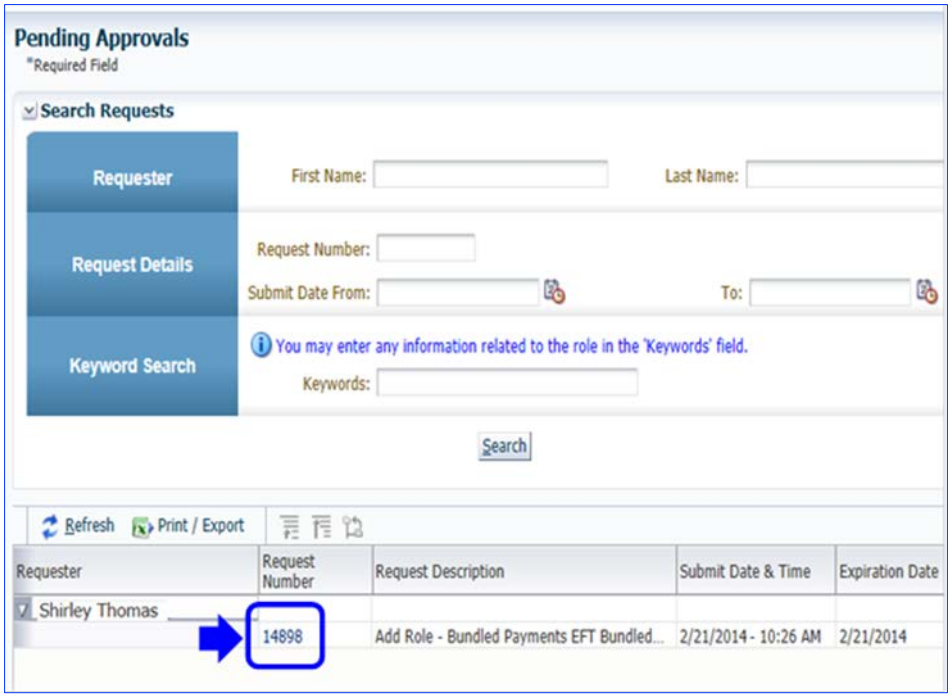
Action
Requester's name for the request that you would like to review.



Step 6 After selecting the single right arrow icon that appears before the Requester's name, the **Request ID** number is displayed.

Select the **Request Number** to open and review the request.

In the example below, we will be selecting Request Number 14898 to open and view this request.



Step 7 The **Approve/Reject Request** page is displayed.

Action

- If the request should be *approved*, enter a justification for the approval in the **Justification for Action** box and select **Approve** to approve the request. All information entered into the **Justification for Action** box will be included in the E-mail sent to the requester.
- If the request should be *rejected*, enter a justification for the rejection in the **Justification for Action** box and select **Reject** to reject the request. All information entered into the **Justification for Action** box will be included in the E-mail sent to the requester.
- If the request should be *deferred* and no action taken, select **Defer** to defer the request and the pending request will remain on the **My Pending Approvals** page for all of the application's authorized approvers. Do not enter any information in the **Justification for Action** box, if you are deferring a request. Any information entered in the **Justification for Action** box will not be saved for deferred requests.

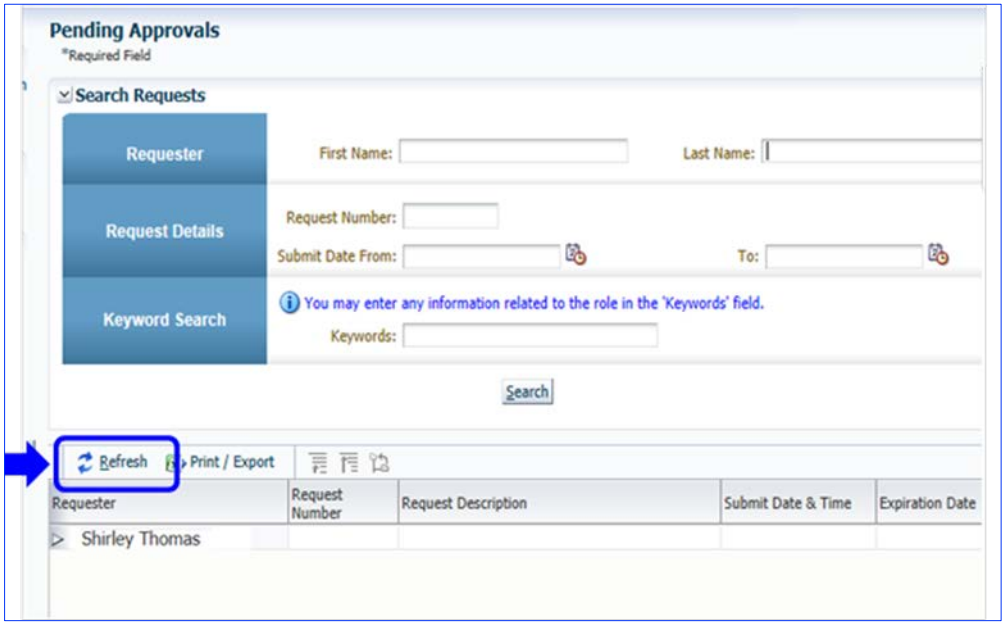
In the example below, the request should be approved. We will enter the justification in the **Justification for Action** box and select **Approve**.

Action	
Step 8	After selecting **Approve**, you will be sent back to your **Pending Approvals** page.

Note:

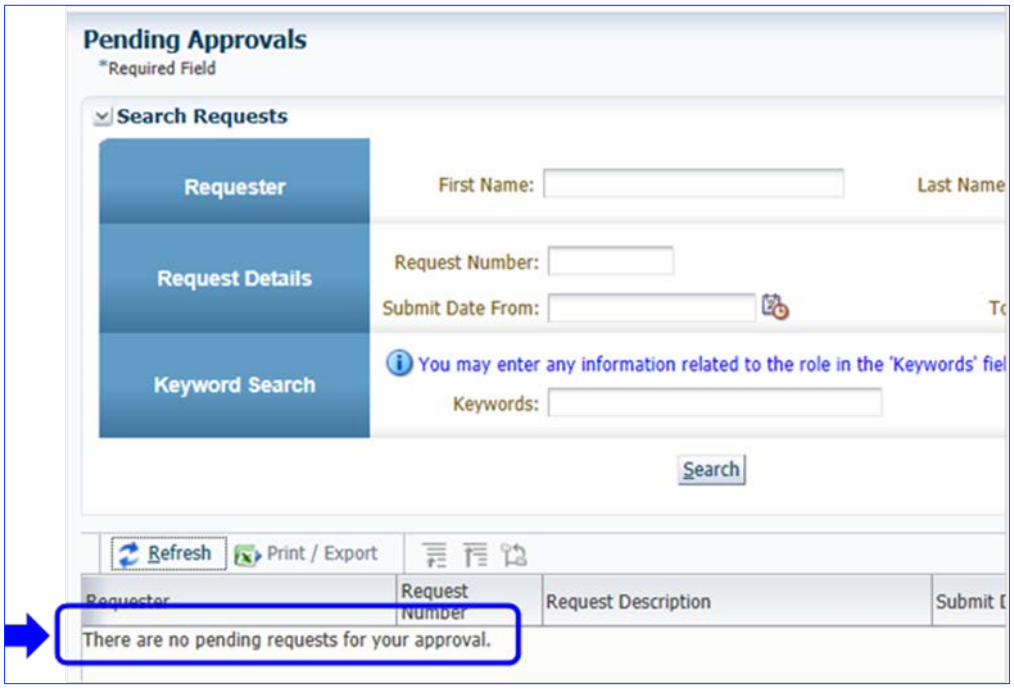
The pending request will still be displayed on your Pending Approvals page until you select Refresh.

Select **Refresh** to refresh the page.



Step 9	After selecting **Refresh**, the pending request that you have just approved will no longer be displayed.

Action


Pending Approvals
*Required Field
Search Requests
Requester
First Name:
Last Name
Request Details
Request Number:
Submit Date From:
Keyword Search
You may enter any information related to the role in the 'Keywords' fiel
Keywords:
Search
Refresh
Print / Export
Request Number
Request Description
There are no pending requests for your approval.

Pending Approvals

The **Pending Approvals** hyperlink for the applications listed below is located in the **My Actions** view on the CMS Portal home page and can be accessed by EIDM users that have Approval authority.

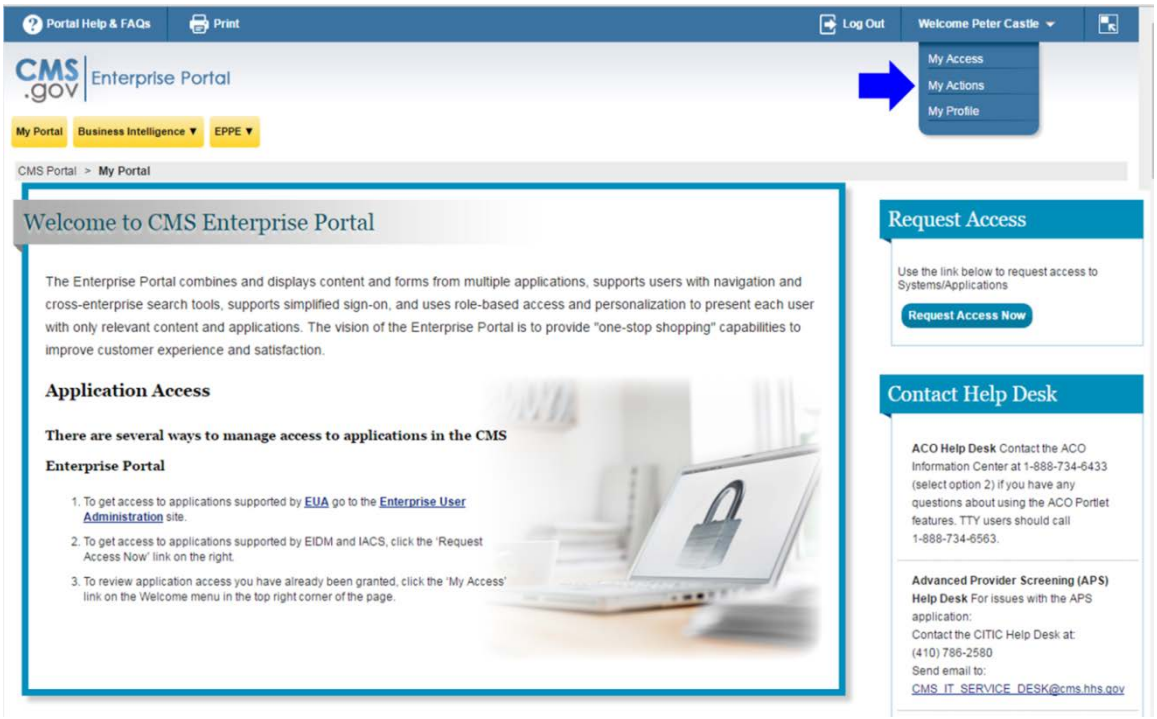
To find, review, approve, reject, or defer a pending request for one of these applications,

Applications	
• ASETT	• MCU
• ASP	• MLMS
• EPPE	• Open Payments
• ESD	• SHIM
• IC	• T-MSIS
• DHD	• zONE
• MACPro	

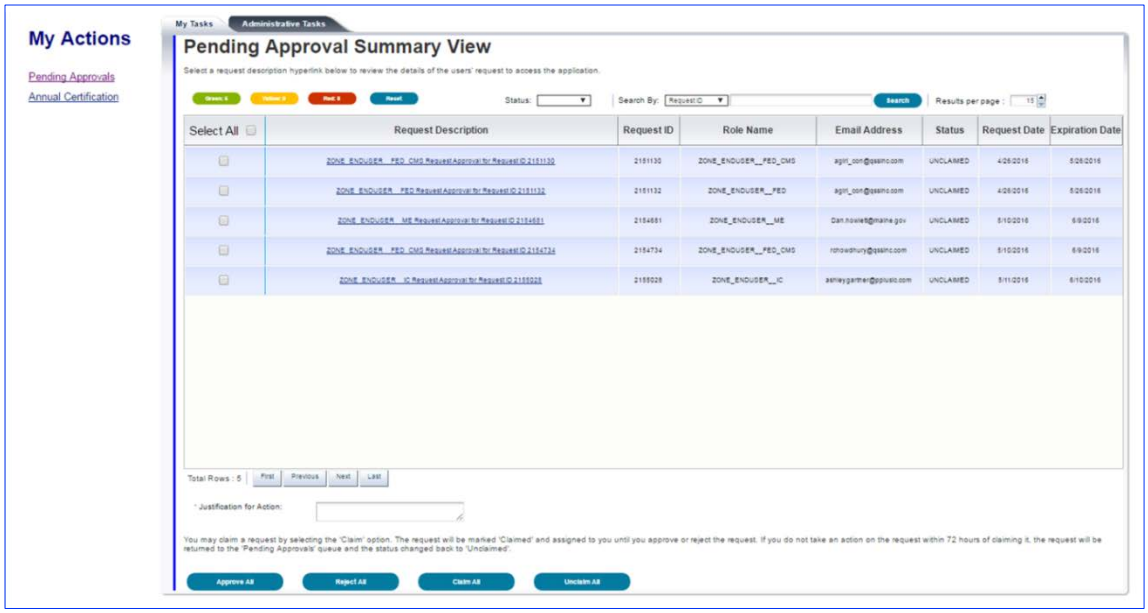
Please **FOLLOW THESE STEPS**.

	Action
Step 1	After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed. Select the drop-down list located on the top right corner of the Portal home page and Select the **My Actions** link.

Action



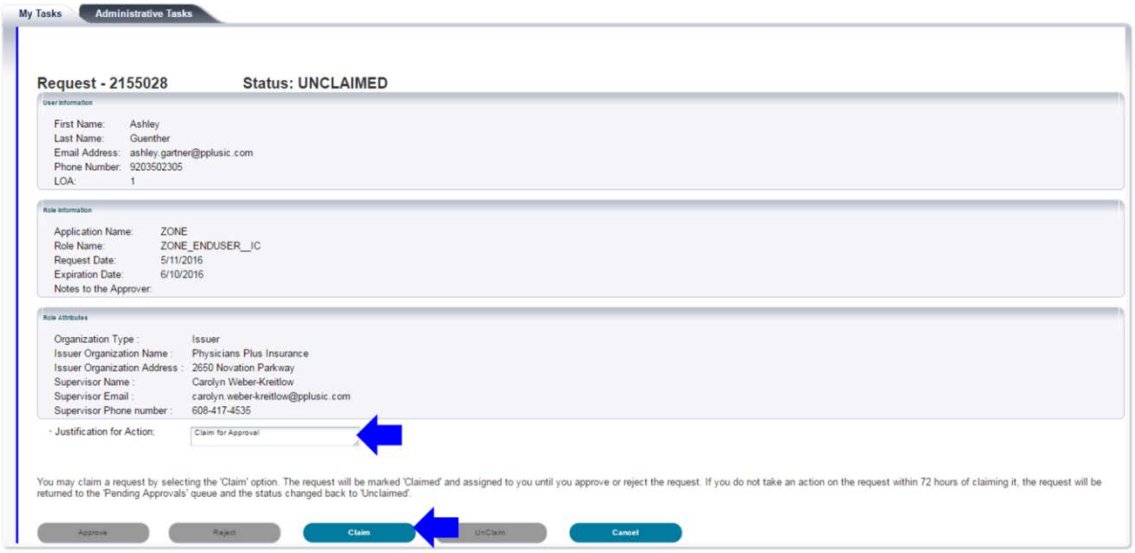
Step 2 The **My Actions** page will display the **Pending Approval Summary View**, and the pending approvals queue as shown in the figure below.



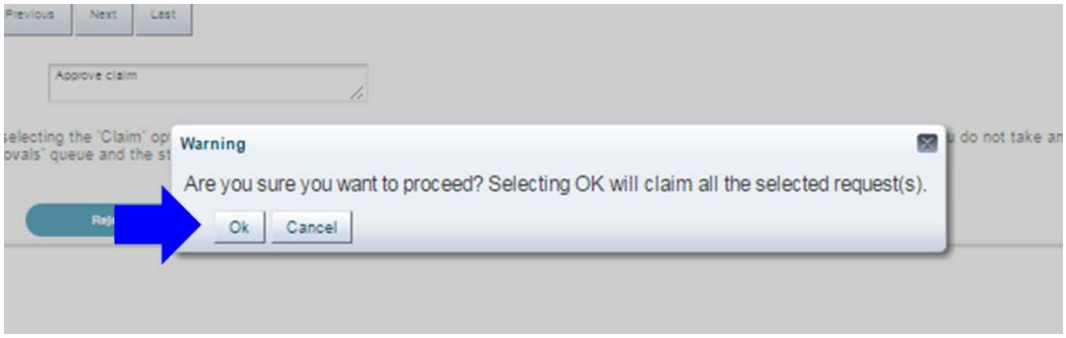
Step 3 Claim the approval request by selecting the **Request Description** hyperlink of the Request ID you wish to claim in the **Pending Approval Summary**.

Action

Step 4 In the **Status: UNCLAIMED** window enter a justification for claiming the request in the **Justification for Action** field at the bottom of the page. Select the **Claim** button to continue.

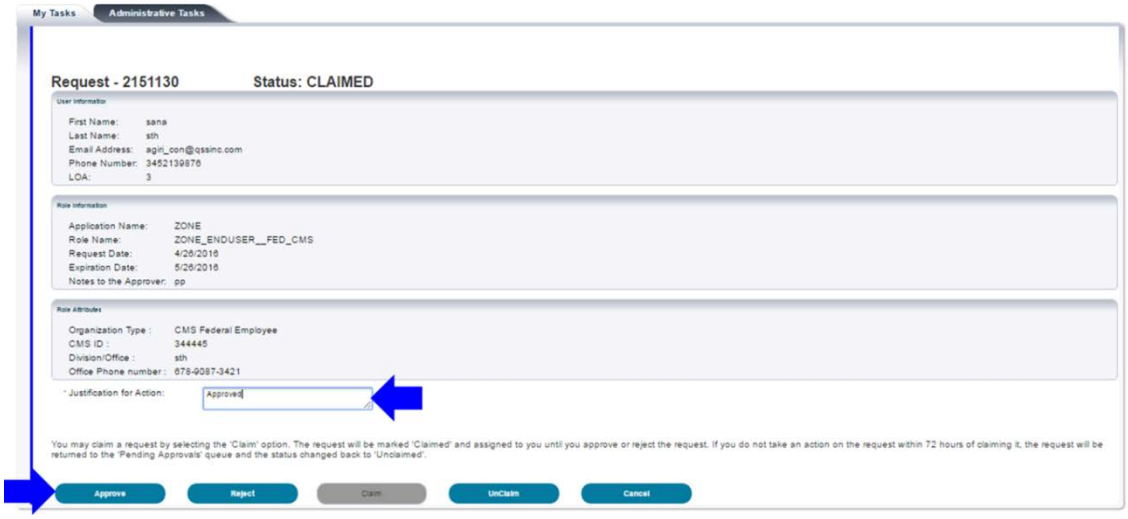


Step 5 Select **Ok** to claim the selected request, or Cancel to cancel the action and return to the Pending Approval Requests Summary screen.

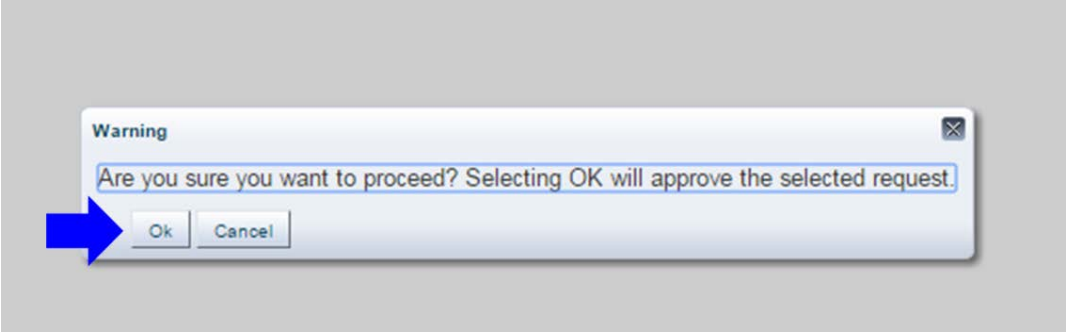


Action

Step 6 In the **Status: CLAIMED** window, enter a justification for your action in the **Justification for Action** field at the bottom of the page. Select **Approve** or **Reject** to approve or reject the claim. Select **Unclaim** to unclaim the request and return it to the **Pending Approval Summary** queue.



Step 7 Select **Ok** to approve the selected request.



Note:

Requests that are approved or rejected will be removed from the queue.

The requestor will receive an E-mail with the status of the request. If the request is rejected, the E-mail will include a reason for the rejection.

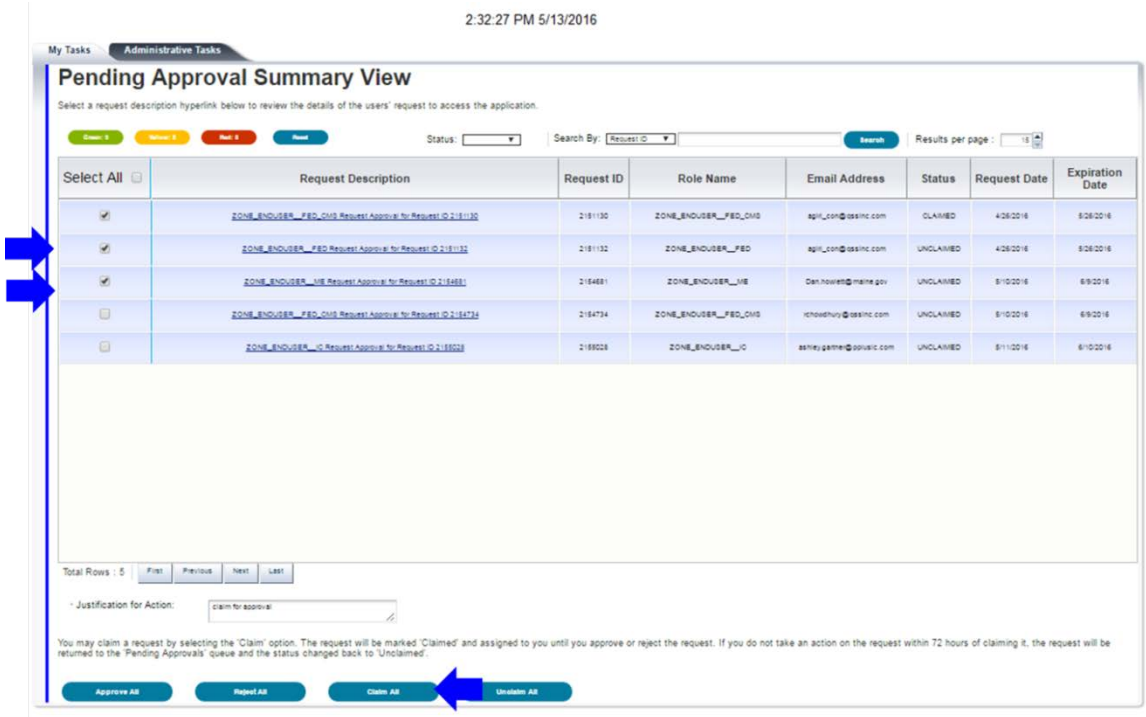
Mass Approval of Pending Requests

To claim multiple pending requests at once for one of the applications below:

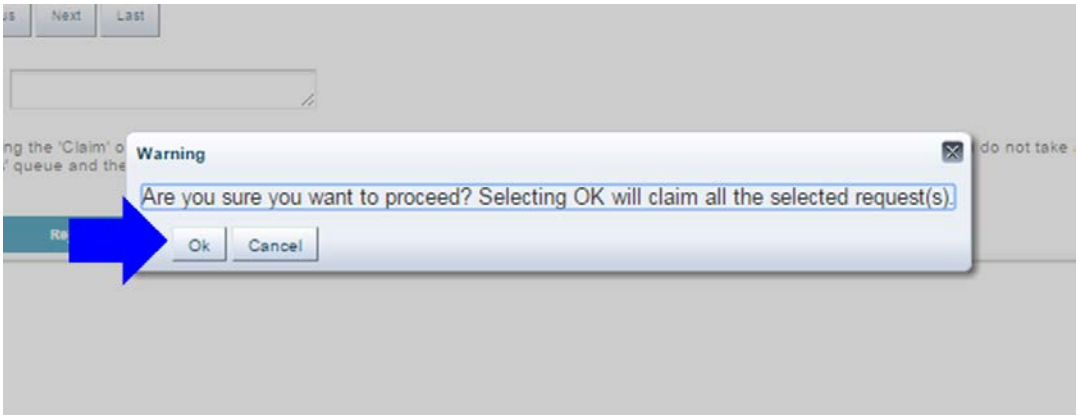
Applications	
• ASETT	• MCU
• ASP	• MLMS
• EPPE	• Open Payments
• ESD	• SHIM
• IC	• T-MSIS
• DHD	• zONE
• MACPro	

Please **FOLLOW THESE STEPS.**

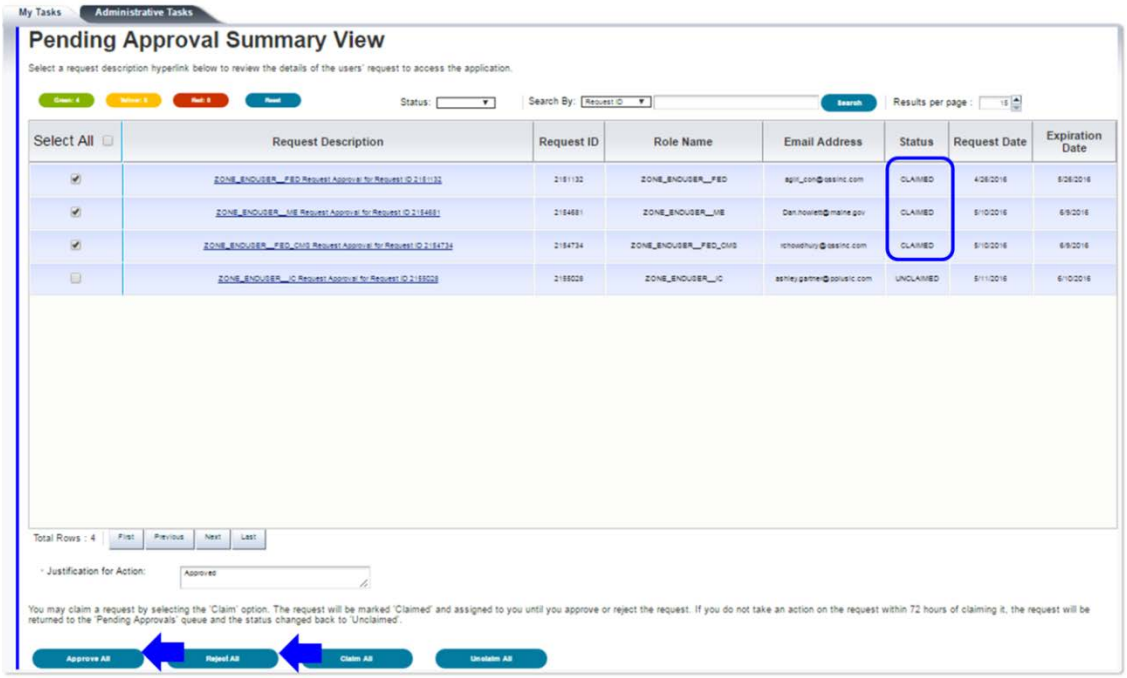
	Action
Step 1	Claim multiple approval requests at once, by selecting the checkboxes next to the Requests you wish to claim in the **Pending Approval Summary** queue. Select **Claim All**.



Action	
Step 2	Selecting Ok will claim all the selected requests. Select **Ok** to proceed.

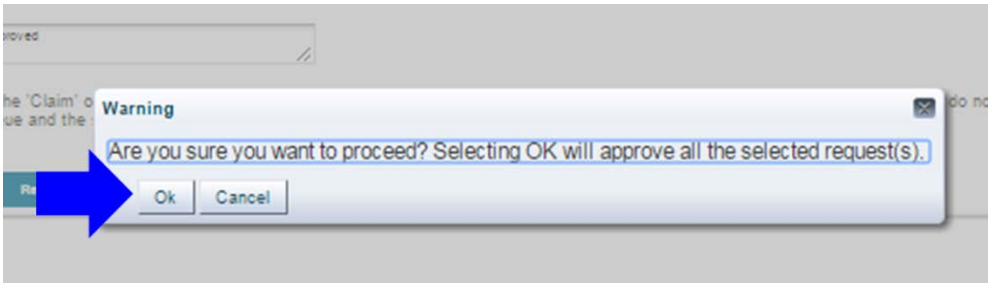


Step 3 The selected requests are now **CLAIMED**. Enter a justification for your action in the **Justification for Action** field at the bottom of the page. Select **Approve All** or **Reject All** to approve or reject the claims. Select **Unclaim** to unclaim the requests.



Step 4 Selecting **Ok** will approve all the selected requests. Select **Ok** to proceed.

Action



Step 5 You will receive a notification that the selected role requests are successfully approved.

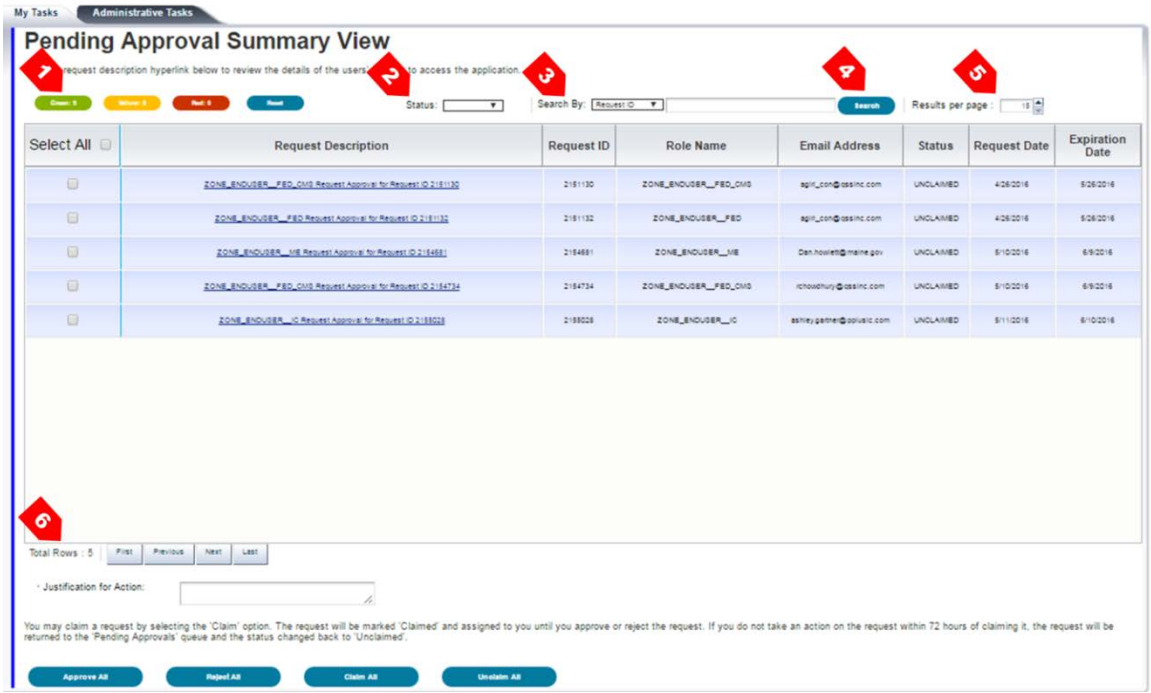
Features of the Pending Approval Summary Dashboard

The Features of the Pending Approval Summary Dashboard listed numerically below are displayed in the screen image that follows.

1. **Color Status indicators**:
   - Green – Displays the number of pending requests that will expire in 21-30 days
   - Yellow – Displays the number of pending requests that will expire within 11-20 days
   - Red – Displays the number of pending requests that will expire within 10 days
   - Reset – Displays all pending requests
2. **Status** search option: - Search by status of pending claims (Claimed, Unclaimed)
3. **Search by** search option - Search by E-mail or Request ID
4. **Search -** Displays the search results
5. **Results per page** – Allows the user to select the number of results that will be displayed.

Action

6. **Total Rows and First, Previous, Next, Last** – Provides easy navigation through multiple pages.



Note:

The approver can only claim a request that is in unclaimed status. The Approver must enter a reason in the Justification for Action field.

The user can exit the My Actions view by selecting the Logout button or exiting the browser.

4. Annual Certification

As of January 2016, enforcement of the Annual Certification requirement for all Applications supported by Enterprise Identity Management (EIDM) is in effect.
Annual Certification is the annual recurrence of the role approval process. Role approval is 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.
CMS.gov provides a means to record the Annual Certification actions taken for two types of roles:

a. **Manually Approved Roles** - the original role request requires manual approval by the user with appropriate authorizing role.
b. **Validated Roles (auto-approved)** - the original role request requires that EIDM compare and validate user provided data to data maintained in a trusted resource (validation check).

When a role fails certification, it is removed from the user's profile.

a. Manually approved roles can fail certification either because the Approver selected 'Revoke' for the user's role, or because the Approver took no action prior to the Annual Certification due date.
b. Validated roles can fail because the user provided data does not match the data in the trusted resource on the Annual Certification due date.

The Annual Certification due date is the date that a Role is due to be certified. Annual Certification is not a certification of a User Identifier (UID) or a User's account.

a. The Annual Certification due date for manually approved roles is one year after the create date for the first certification and one year after the certification date each year thereafter.
b. The Annual Certification due date for Validated Roles is June 1 every year.

The Annual Certification process for any given role is the sole responsibility of the Application and their Approvers. This section explains the Approvers' responsibility regarding Annual Certification for both manually approved and validated roles.

Certifying Manually Approved Roles

Approvers for manually approved roles will have the ability to search for, certify, or revoke the roles assigned to the users under their authority at any time they choose, via the **Annual Certification** page. However, if they do not take an action by the certification due date, then their users' role(s) will be removed.

This section lists step-by-step instructions that an Approver should take in order to certify or revoke their users' access as part of Annual Certification.

The certification process is initiated with an e-mail notification to the Approver:

a. An Approver for manually approved roles will receive an email notifying them that users under their authority are pending Annual Certification. The email will provide instructions for completing the certification for users under their authority.

b. The initial e-mail will be sent 30 days prior to the certification due date for users requiring manual approval.

c. Reminder e-mails will continue to be sent to the Approver 15 days, seven (7) days and one (1) day prior to the certification date.

To certify manually approved roles for Annual Certification, **FOLLOW THESE STEPS:**

	Action
Step 1	Review the email notification that lists the number of roles pending certification. Follow the instructions in the email to access the **Pending Certifications** page to certify users' access. A sample email is shown below.

From: <donotreply@cms.gov>
Date: Fri, Nov 20, 2015 at 4:29 PM
To:
Subject: Action Required: CMS.gov Users' Pending Annual Certification.

This is to inform you that some of your users in the <Application Name> Application for which you are responsible are due for Annual Certification of their roles.

You have 237 roles pending certification in the next 30 days.
You have 210 roles pending certification in the next 15 days.
You have 203 roles pending certification in the next 7 days.
You have 0 roles pending certification in the next 1 day.

To review the pending certifications, please do the following:

1. Login to CMS.gov using the link given below.
2. Navigate to the page where you approve role requests.
3. Select the 'Annual Certification' link.
4. In the 'Pending Certification' view select the user for whom you wish to take an action. If you do not find the user in the 'Pending Certification' view, select the 'Search Users' tab to search for the user.
5. 'Certify' the user if you wish to retain the user's role in the application.
6. 'Revoke' the user if you wish to remove the user's role in the application. This will be effective immediately.

Note: If you fail to take any action, the users' role(s) will be removed on the certification due date for that role(s).

If you are accessing CMS.gov from CMS Net, Go to <CMS NET URL>.
If you are accessing CMS.gov from the Internet, Go to <Internet URL>.

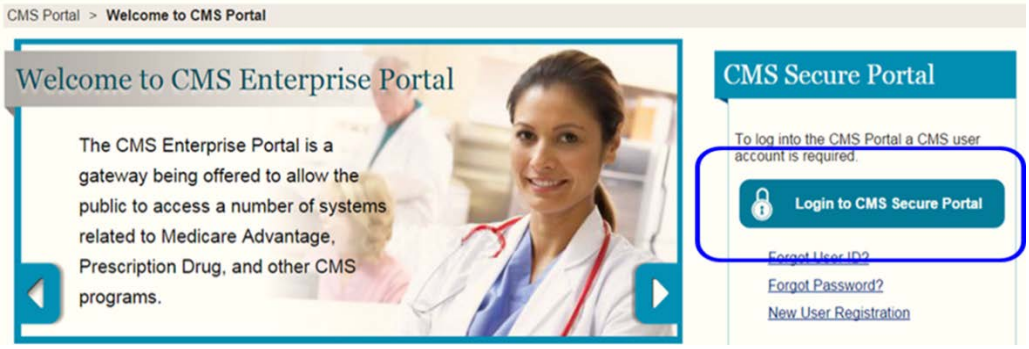
Thank you,
CMS.gov
Please do not reply to this system-generated E-mail.

Action

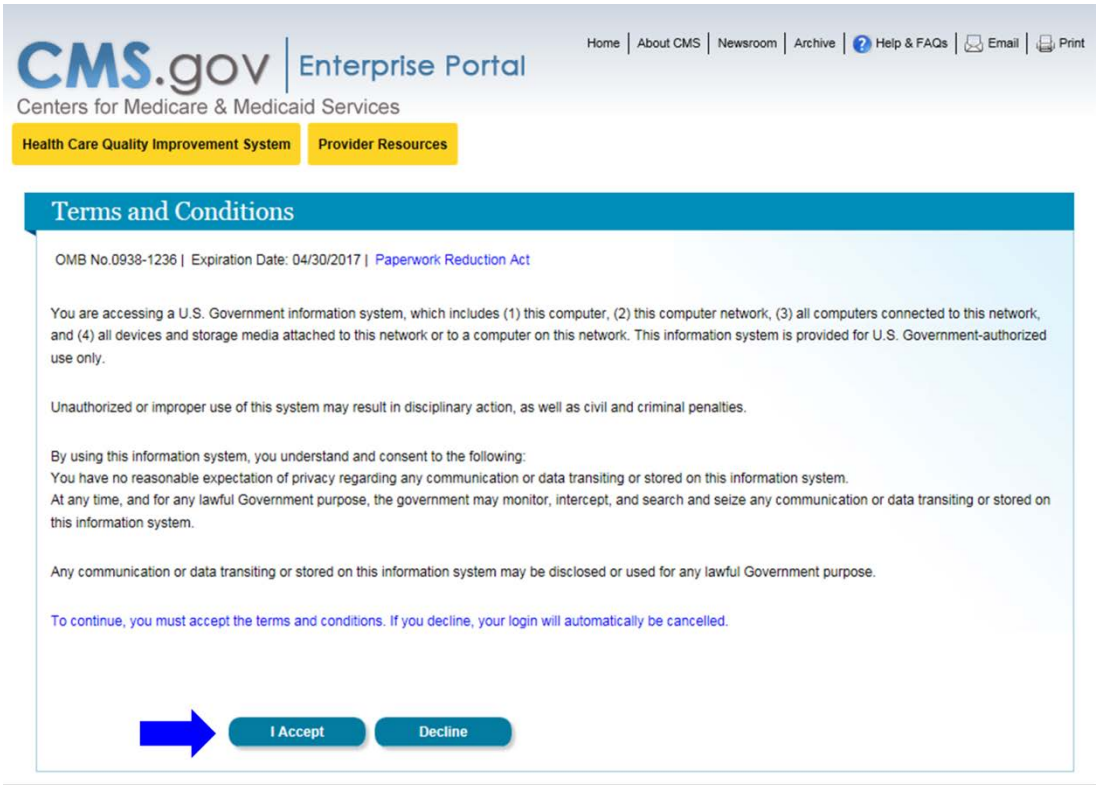
Note:

The 'roles pending certification' requests listed in the e-mail will provide the number of pending certifications that require action in the specified number of days.

Step 2 Go to https://portal.cms.gov/ and select **Login to CMS Secure Portal**.

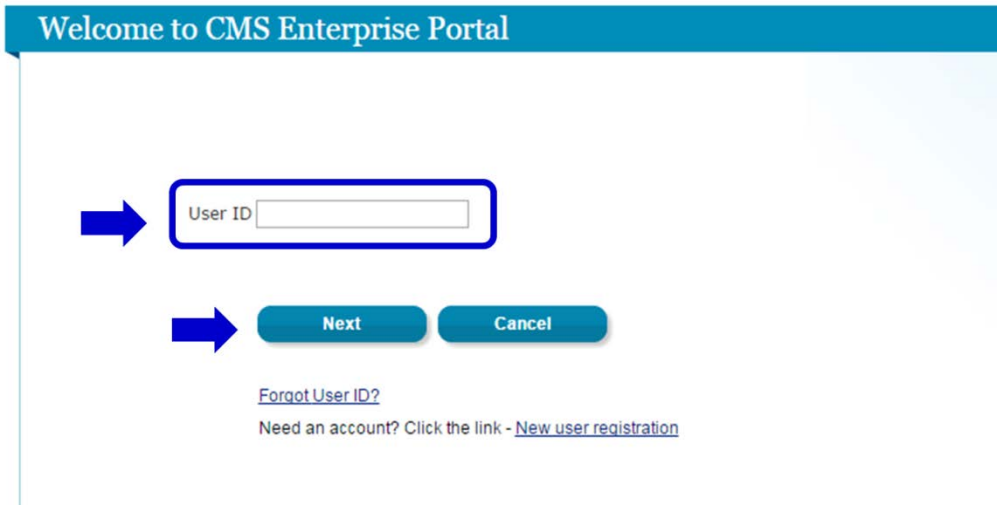


Step 3 Read the **Terms and Conditions** and select **I Accept** to continue.

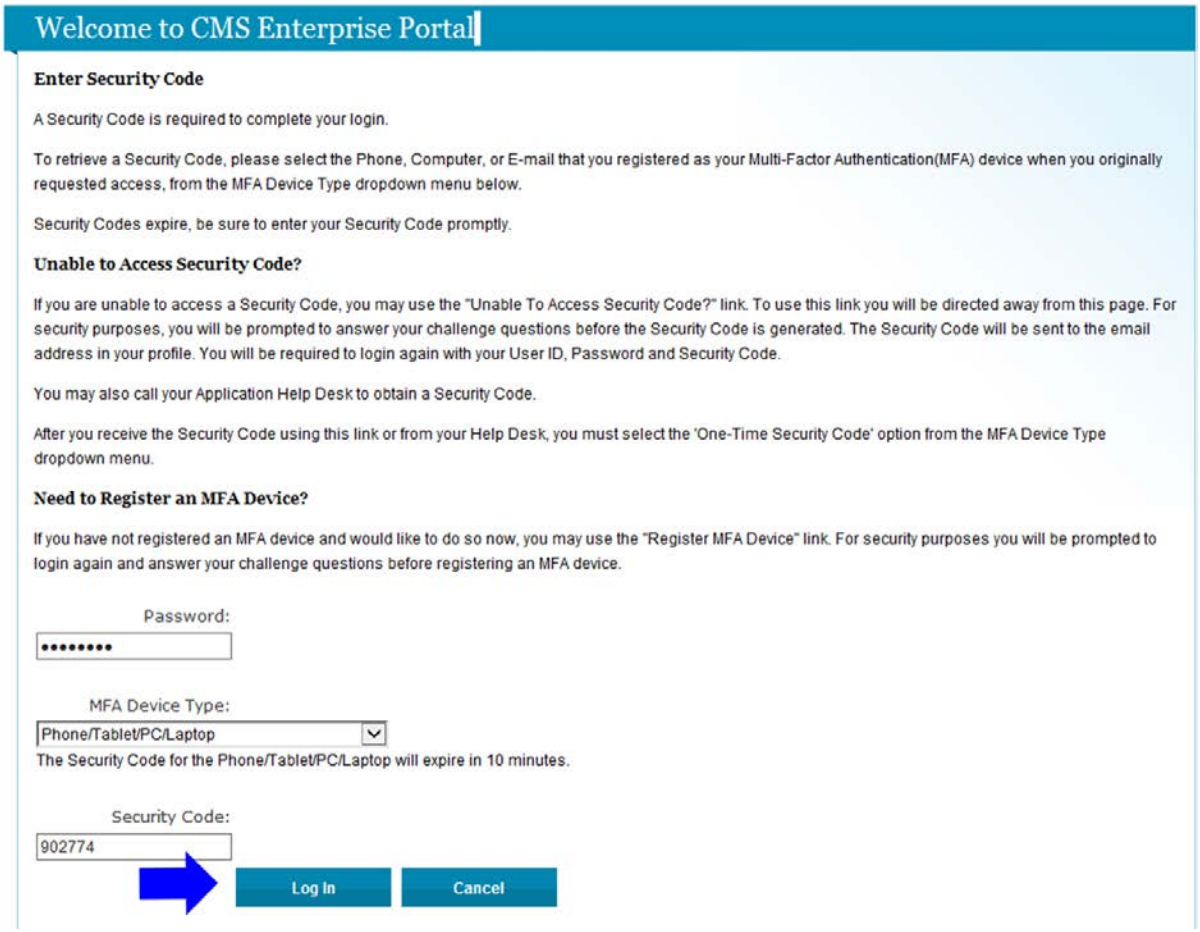


Step 4 Enter your User ID Select **Next** to continue.

Action



Step 5 Enter your Password, MFA Device Type, and Security Code. Select **Log In**.

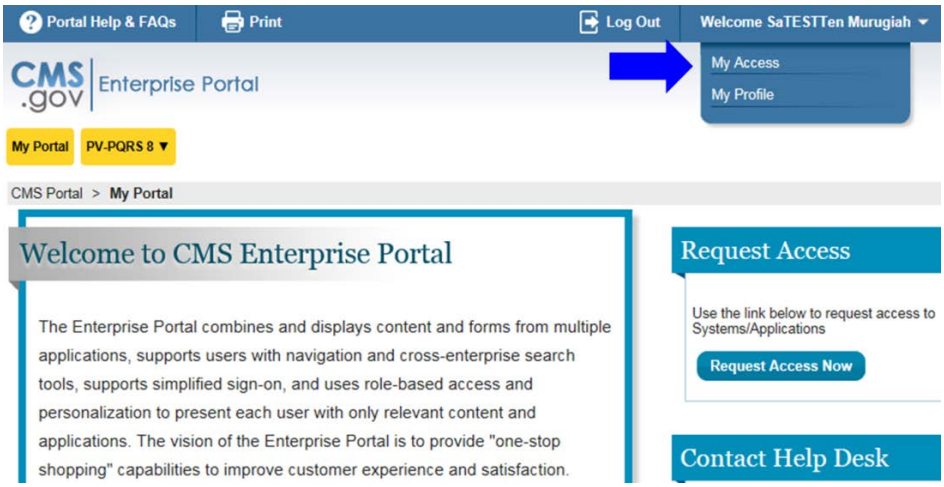


Action

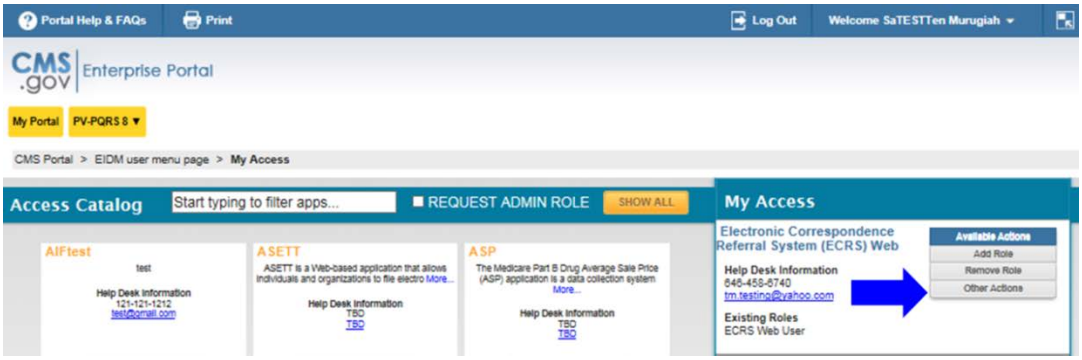
Note:

For more information on Multi-Factor Authentication (MFA) please refer to the **CMS EIDM User Guide**.

Step 6 Select **My Access** in the drop down menu at the top right corner of the Welcome screen.

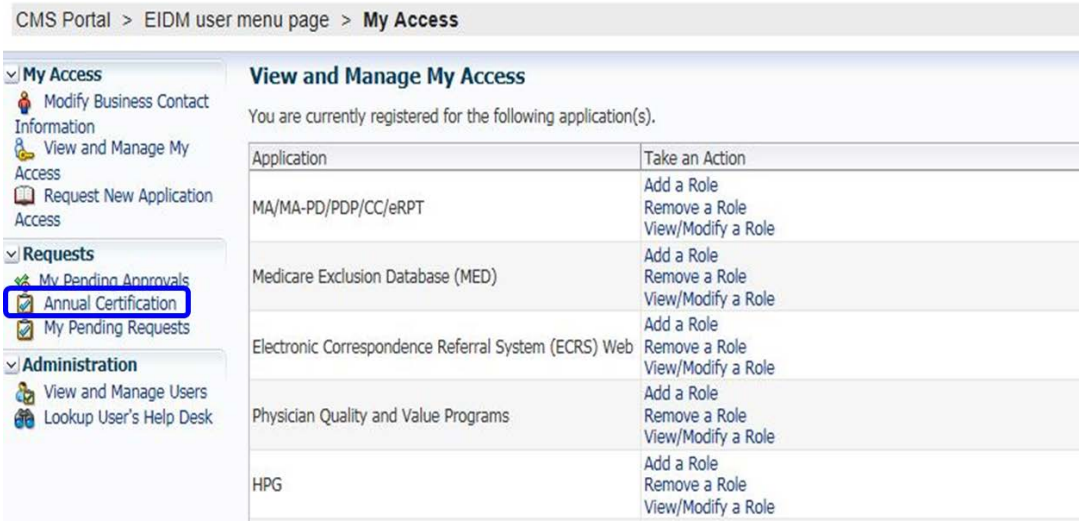


Step 7 Select **Other Actions** on the **My Access** page.



Step 8 On the **View and Manage My Access** page. Select the link for **Annual Certification** on the left pane.

Action

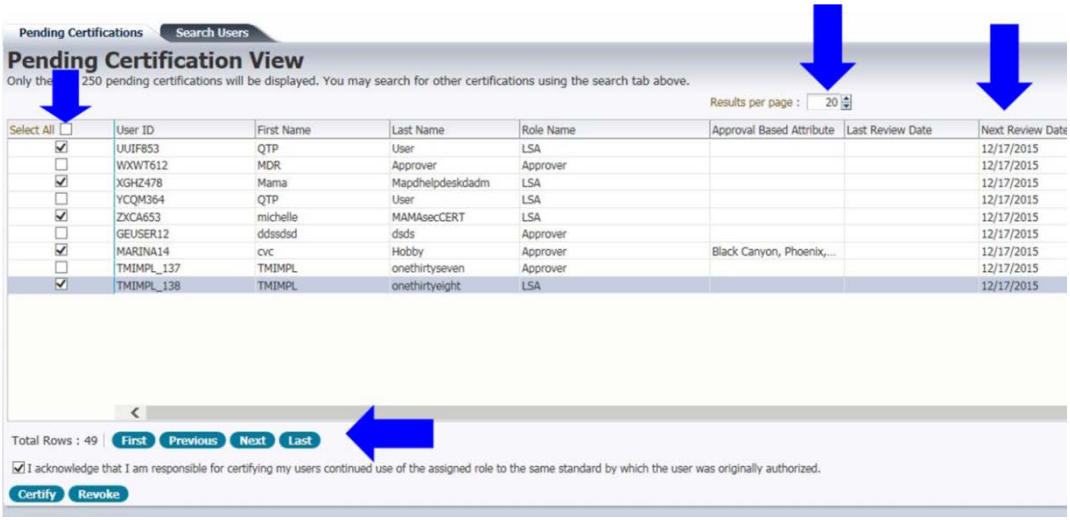


Step 9

In the **Pending Certification View**, select users one by one or in bulk (by selecting the **Select All** button) to **Certify** or **Revoke** users' roles.

Only users whose roles are due for certification within the next 30 days will be shown initially.

Use the **Search Users** tab to search for users outside the 30 day window or to search for a specific pending certification by User ID, User name, etc.



Action

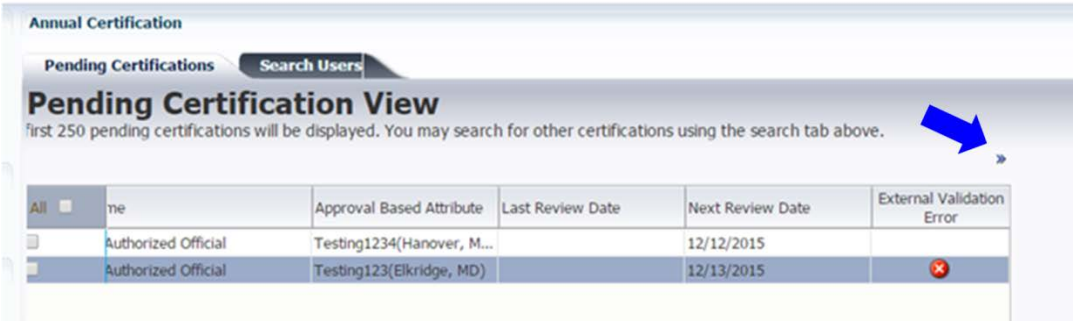
Note:

By default, the pending certifications display up to 250 results and are sorted in descending order by the Next Review Date column. The Approver can sort the pending certifications using the fields along the columns.

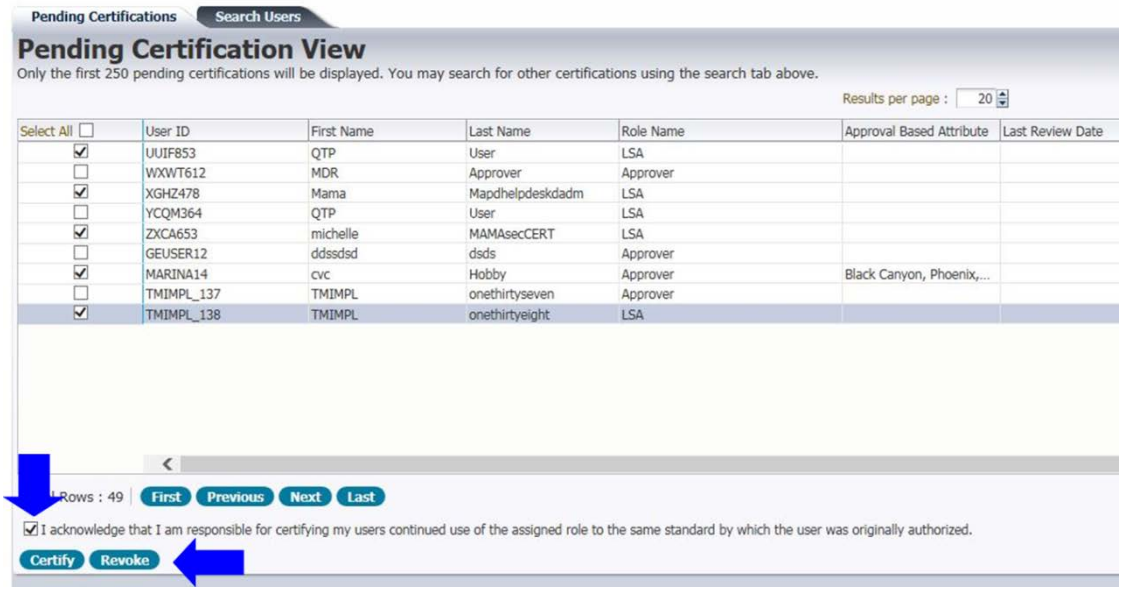
The system uses pagination when displaying results. The ability to toggle through pages can be utilized by selecting First, Previous, Next and Last.

Use the Results per page to display up to 30 results per page. By default it will be set to 15.

Step 10 Select the double arrow in the top right corner to expand the table view to see all populated columns.



Step 11 Agree to the acknowledgement statement to certify or revoke the selected user(s). Select **Certify** or **Revoke** to complete the pending user's role certification.



Action

Note:

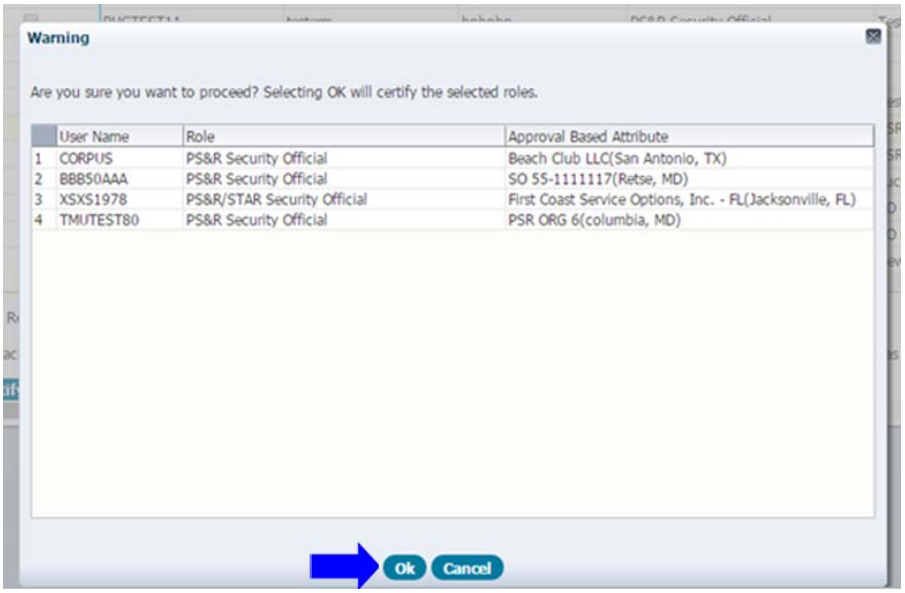
The **Certify** button approves the annual certification of the user's use of a role in an application.

The **Revoke** button removes the user's role from the application. The user will be notified via e-mail when a role is revoked.

Step 12 A pop-up confirmation message will appear providing the list of users included for that action.

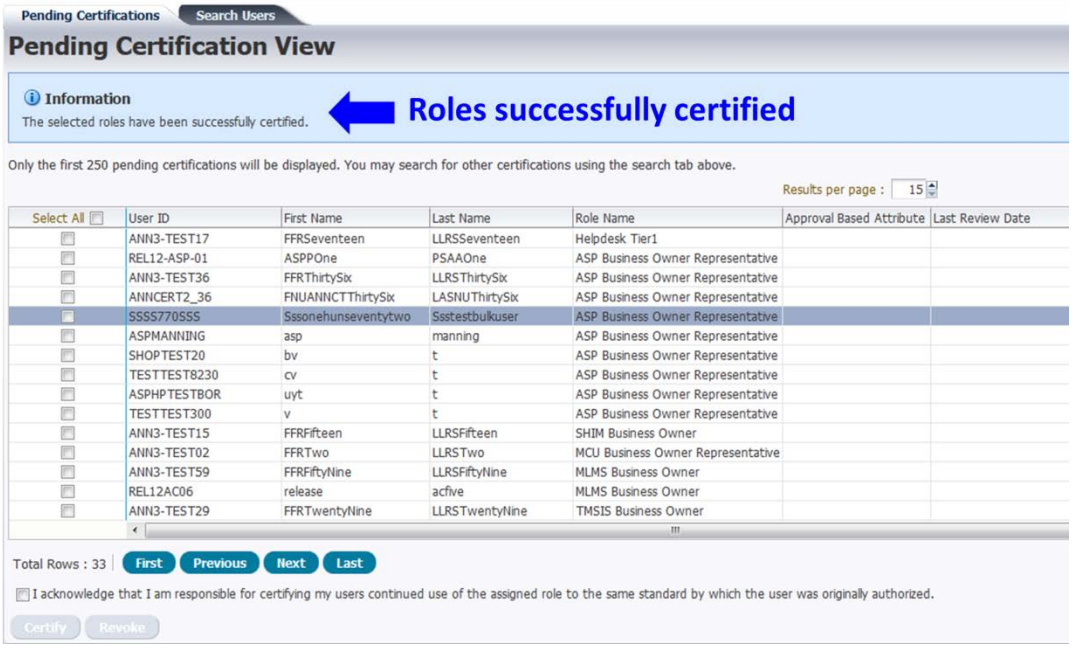
Review the User ID, role, and Approver-based information of the pending certifications that are going to certified or revoked.

Confirm the action by selecting the **Ok** button. Select the **Cancel** button to cancel the action and to return to the **Search Users View** page.

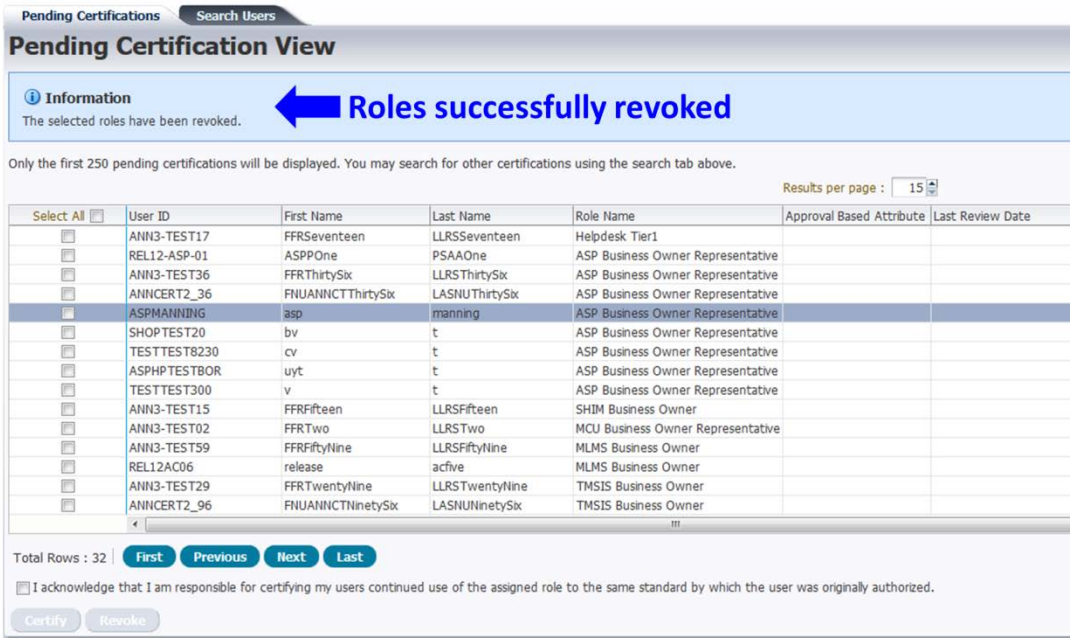


Step 13 After certifying or revoking the roles, a notification will be displayed in the **Pending Certification View** confirming that the roles have been **Certified** or **Revoked**.

Action



Select All	User ID	First Name	Last Name	Role Name	Approval Based Attribute	Last Review Date
	ANN3-TEST17	FFRSeventeen	LLRSSeventeen	Helpdesk Tier1		
	REL12-ASP-01	ASPPOne	PSAAOne	ASP Business Owner Representative		
	ANN3-TEST36	FFRThirtySix	LLRSThirtySix	ASP Business Owner Representative		
	ANNCERT2_36	FNUANNCTThirtySix	LASNUThirtySix	ASP Business Owner Representative		
	SSSS770SSS	Sssonehunseventytwo	Ssstestbulkuser	ASP Business Owner Representative		
	ASPMANNING	asp	manning	ASP Business Owner Representative		
	SHOPTEST20	bv	t	ASP Business Owner Representative		
	TESTTEST8230	cv	t	ASP Business Owner Representative		
	ASPHPTESTBOR	uyt	t	ASP Business Owner Representative		
	TESTTEST300	v	t	ASP Business Owner Representative		
	ANN3-TEST15	FFRFifteen	LLRSFifteen	SHIM Business Owner		
	ANN3-TEST02	FFRTwo	LLRSTwo	MCU Business Owner Representative		
	ANN3-TEST59	FFRFiftyNine	LLRSFiftyNine	MLMS Business Owner		
	REL12AC06	release	acfive	MLMS Business Owner		
	ANN3-TEST29	FFRTwentyNine	LLRSTwentyNine	TMSIS Business Owner		



Select All	User ID	First Name	Last Name	Role Name	Approval Based Attribute	Last Review Date
	ANN3-TEST17	FFRSeventeen	LLRSSeventeen	Helpdesk Tier1		
	REL12-ASP-01	ASPPOne	PSAAOne	ASP Business Owner Representative		
	ANN3-TEST36	FFRThirtySix	LLRSThirtySix	ASP Business Owner Representative		
	ANNCERT2_36	FNUANNCTThirtySix	LASNUThirtySix	ASP Business Owner Representative		
	ASPMANNING	asp	manning	ASP Business Owner Representative		
	SHOPTEST20	bv	t	ASP Business Owner Representative		
	TESTTEST8230	cv	t	ASP Business Owner Representative		
	ASPHPTESTBOR	uyt	t	ASP Business Owner Representative		
	TESTTEST300	v	t	ASP Business Owner Representative		
	ANN3-TEST15	FFRFifteen	LLRSFifteen	SHIM Business Owner		
	ANN3-TEST02	FFRTwo	LLRSTwo	MCU Business Owner Representative		
	ANN3-TEST59	FFRFiftyNine	LLRSFiftyNine	MLMS Business Owner		
	REL12AC06	release	acfive	MLMS Business Owner		
	ANN3-TEST29	FFRTwentyNine	LLRSTwentyNine	TMSIS Business Owner		
	ANNCERT2_96	FNUANNCTNinetySix	LASNUNinetySix	TMSIS Business Owner		

Action

Note:

The view screen will refresh and the Next Review Date will be updated for users whose roles were certified.

The users' roles that were revoked will no longer be included in the pending certifications list.

Users whose role(s) were removed by the revoke action will receive an email with instructions to regain access to the application.

The email will include Application Help Desk contact information for the application in which the user had the role.

Using the 'Search Users' Feature

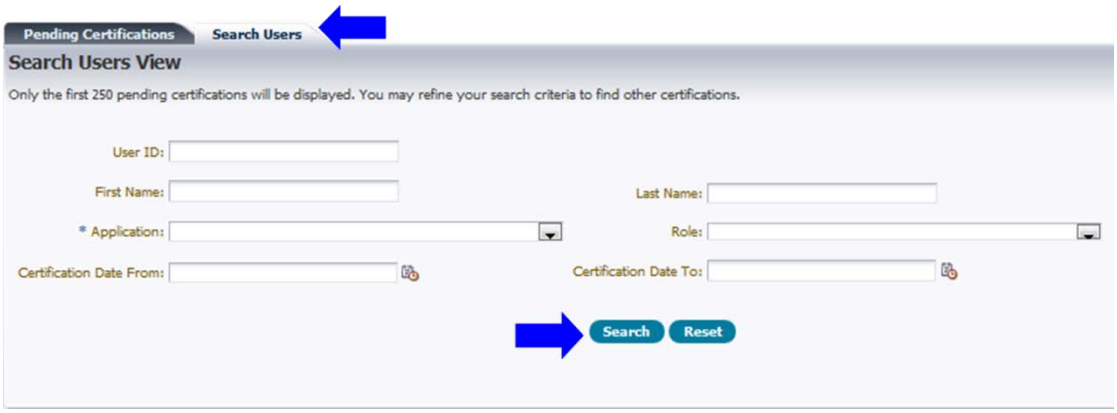
Approvers can select the **Search Users** tab to search pending certifications for users' roles under their approval authority. Users whose roles are due for certification matching the search criteria will be populated in the search results.

To use the Search Users feature, **FOLLOW THESE STEPS**:

Action

Step 1 Search pending certifications for users' roles by providing the search criteria on the **Search Users View** page.

Select **Search** to retrieve a list of users matching the search criteria. To clear the search criteria, select the **Reset** button.



Action

Note:

The following characters are not allowed in any of the search fields: Asterisk (*), Percentage (%), Double quotation mark (“), Ampersand (&), Cap (^), Less-than sign (<), and Greater-than sign (>).

User ID, **First Name**, and **Last Name**: Enter a minimum of 2 characters in the search field.

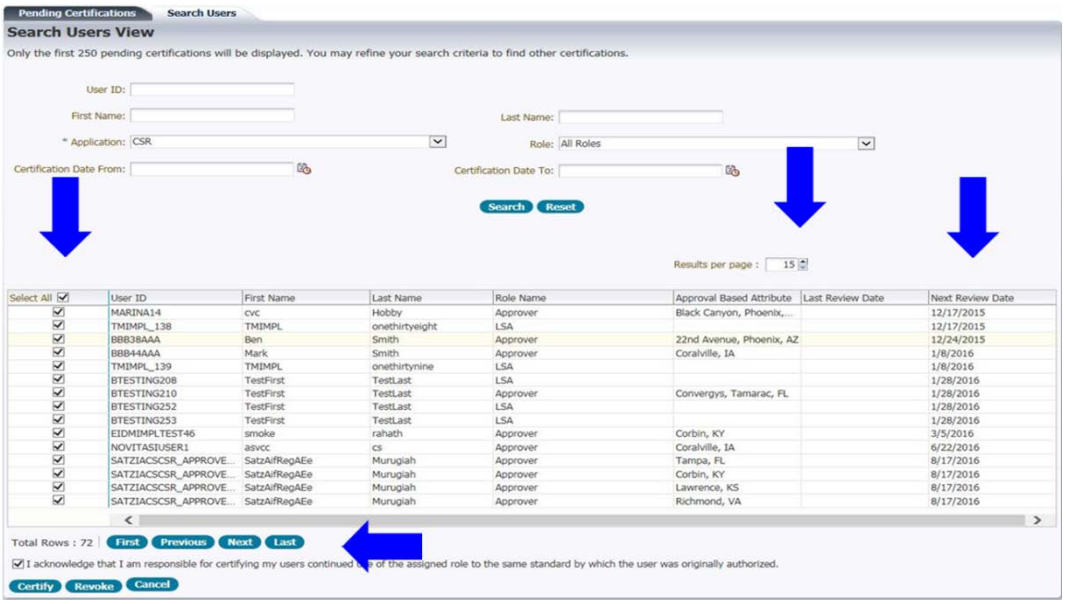
Application: If you are an approver for only one application, the application name will be pre-selected by default and will be grayed out.

Application: This is a mandatory field if you are an approver for *more than* one application. Please select the application.

Role: This is an optional field and displays the roles within the application which are under your approval authority. If you are an approver for only one role in the application, the role will be pre-selected by default and will be grayed out.

Certification Date From and To: Enter a date in mm/dd/yyyy format, or select a date to search pending certifications. From date cannot be past 365 days from the current date.

Step 2 Review the pending certifications that match your search criteria. Select users one by one or in bulk by selecting the **Select All** button to **Certify** or **Revoke** users’ roles.



Action

Note:

By default, the results are sorted by the Next Review Date column. The Approver can sort the search results using the fields along the columns.

By default, up to 250 results will be populated. All pending certifications that are due up to the next 365 days can be viewed.

The system uses pagination when displaying results. The ability to toggle through pages can be utilized by selecting First, Previous, Next and Last.

Use the Results per page to display up to 30 results per page. By default, it will be set to 15.

The following are the different fields that are displayed in the search results:

User ID, **First Name**, **Last Name**: User information of the user who matches the search criteria.

Role Name: User role for the user who matches the search criteria.

Approval Based Attribute: The role attribute that is provided by the user at the time of role request and is used to identify the Approver and route the request to that Approver.

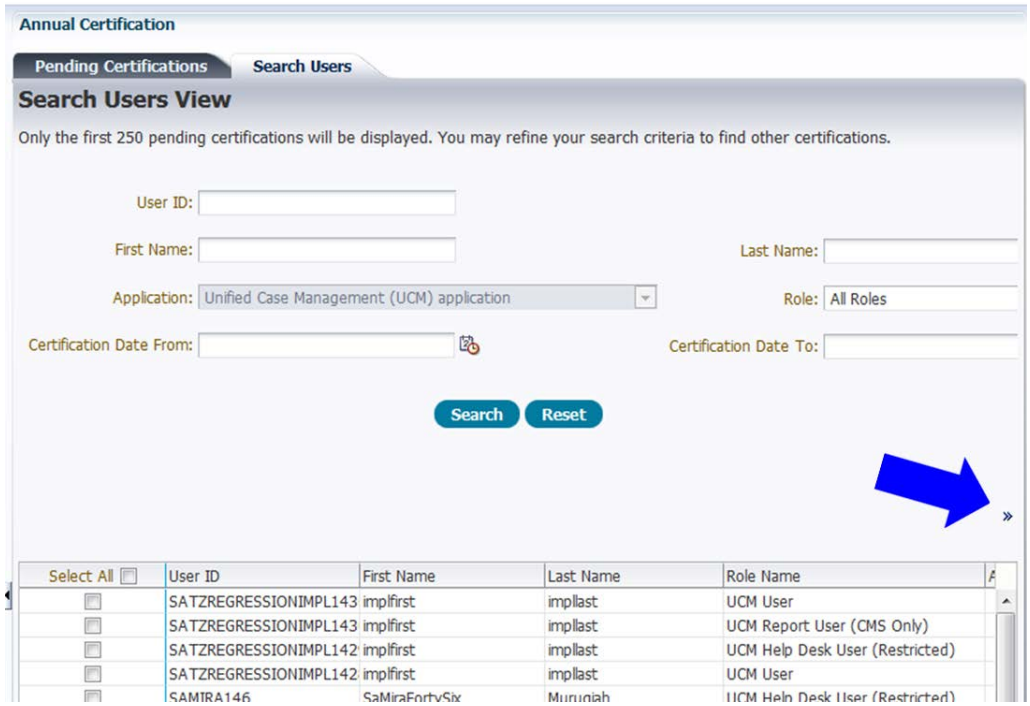
Last Review Date: The last date Annual Certification was completed.

Next Review Date: The next Annual Certification due date.

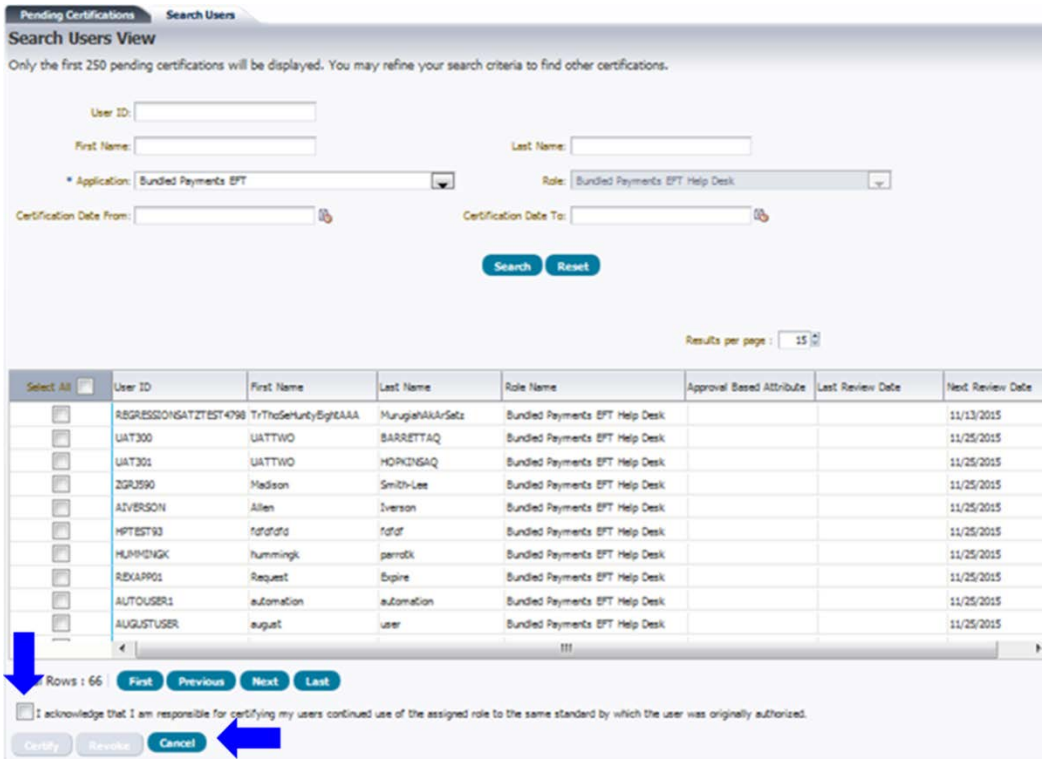
External Validation Error: Only shows for application roles where the original role request required that EIDM compare and validate user provided data to data maintained in a trusted resource that require trusted resource validation. It will be displayed only when the trusted resource validation fails.

Step 3 Select the double arrow in the top right corner to expand the table view to see all populated columns.

Action



Step 4 Agree to the acknowledgement statement to Certify or Revoke the selected user(s). Select **Certify** or **Revoke** to complete the pending user's role certification.



Action

Note:

The **Certify** button approves the annual certification of the user's use of a role in an application.

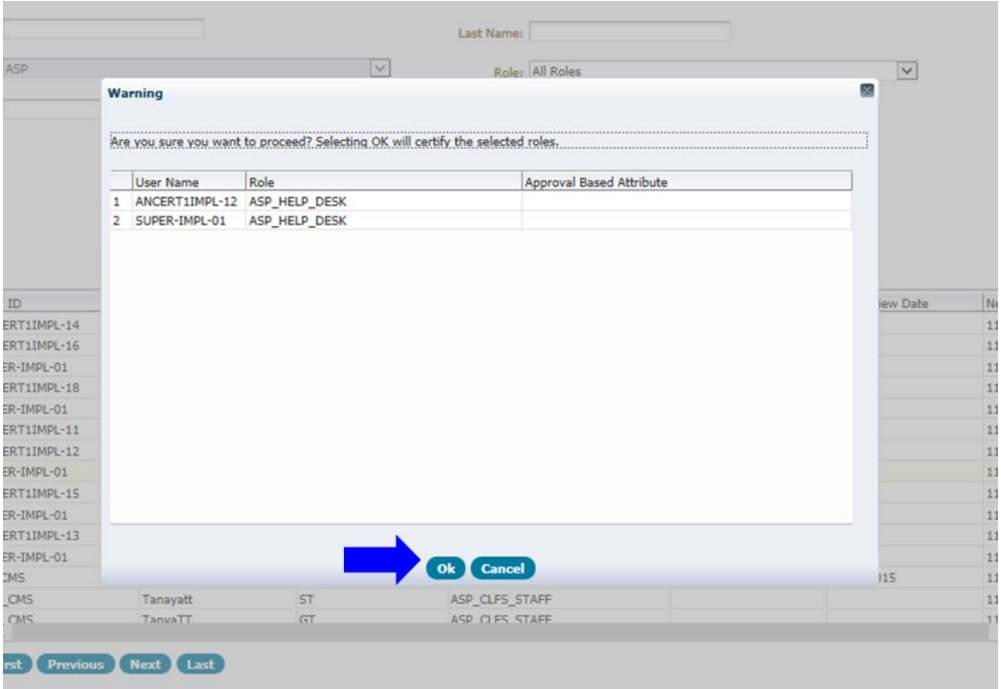
The **Revoke** button removes the user's role from the application. The user will be notified via e-mail when a role is revoked.

The **Cancel** button clears the search and navigates the Approver back to the Pending

Step 5 A pop-up confirmation message provides the list of users included for that action. Review the user IDs, role, and approver-based information of the pending certifications that are going to certified or revoked.

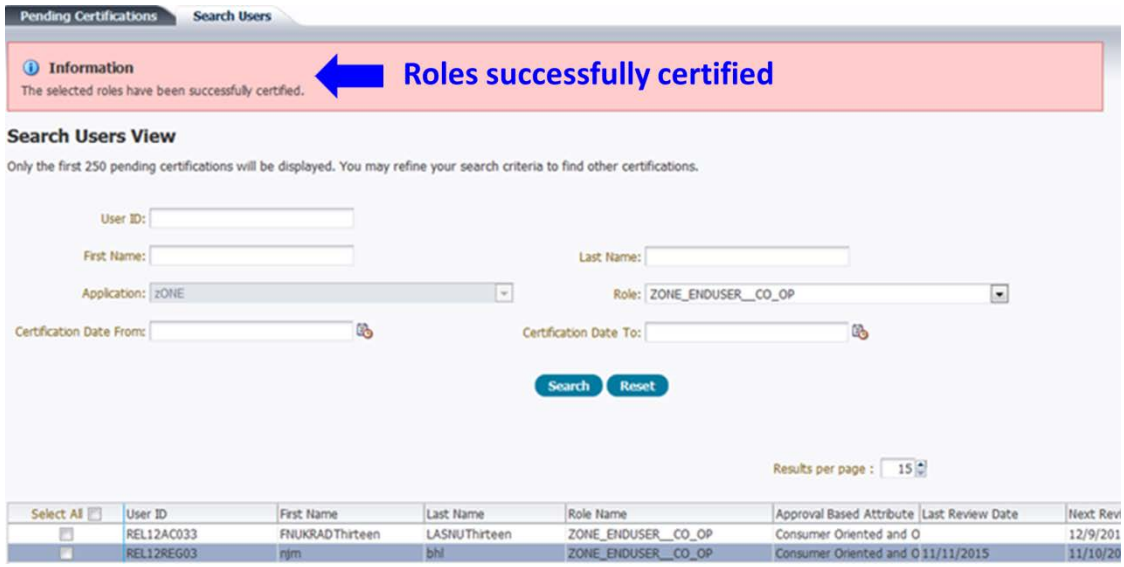
Confirm the action by selecting the **Ok** button.

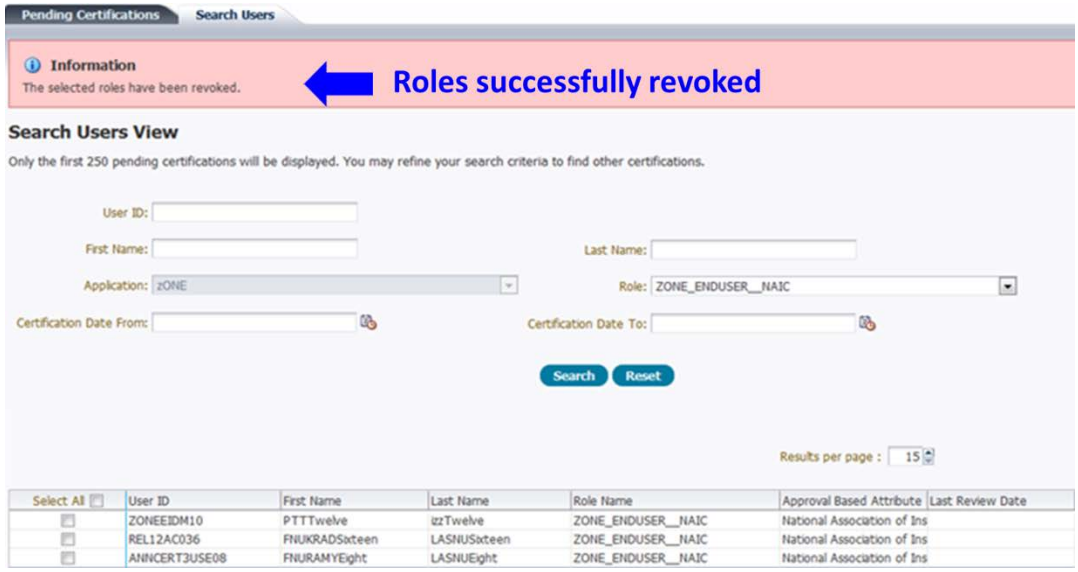
Select the **Cancel** button to cancel the action and to return to the **Search Users View** page.



Step 6 After certifying or revoking the roles, a notification will be displayed in the **Search Users View** confirming that the roles have been **Certified** or **Revoked**.

Action





Note:

The user will receive an email when either the Approver revokes the role access, or when no action is taken by the Annual Certification due date and the system removes the user's role.

Instructions for regaining access to the application are provided in the email.

A sample email is shown below.

Action

From: donotreply@cms.hhs.gov [mailto: donotreply@cms.hhs.gov]

Sent: Monday, October 19, 2015 2:05 PM

To:

Subject: Your CMS.gov Application Role has been removed.

Dear <First Name> <Last Name>,

The Centers for Medicare and Medicaid Services (CMS) require that your Role, <Role Name>, in the <Application Name> Application be approved each year. This email is to notify you that your Application Approver has removed your role.

If you wish to regain access to your application please request the role again by logging into the CMS.gov Enterprise Portal at <portal landing page URL> .

If you need additional assistance contact your <Application Name> Help Desk at <ApplicationHelpdesk email> or call <ApplicationHelpdesk phone number>.

Thank you,

CMS.gov

Please do not reply to this system generated E-mail.

Validated Roles

Validated (auto-approved) roles are certified by the system. An Approver need not take an action in certifying or revoking these roles.
Validated roles require that EIDM compare and validate user provided data (data provided at the time of role request) against the data maintained in a trusted resource (validation check).
When the validation check fails because the user data does not match the data in the trusted resource, an Approver or Business Owner will receive an email notification.
Some examples are shown below:

Users Failed Validation Check – Approver Email Notification

- Approvers who are responsible for users with validated roles will receive the initial email 90 days prior to the Annual Certification due date.
- This email will include the users and roles which failed the validation check.
- Reminder emails will continue to be sent if the user(s) did not pass the validation check 60 days, 30 days, seven days, and one day prior to the Annual Certification due date.
- A sample email is shown below.

From: "donotreply@cms.gov" <donotreply@cms.gov>
Sent: Monday, November 23, 2015 10:06 AM
To:
Subject: Action Required: Your CMS.gov application users' auto approved roles have failed validation

You are receiving this notification because some of your users for which you are either directly or indirectly responsible for, failed an external data source validation as part of Annual Certification. The user details are attached.

Please ensure that the validation data matches for these users. If no corrective action is taken the user(s) will fail Annual Certification and their role(s) will be removed on the certification due date for that role(s)

Thank you,
CMS.gov
Please do not reply to this system generated E-mail.

Note:

- If the user's account failed validation check by the certification due date, their role will be removed and the user will be notified by email.
- If the user's account passed validation check, then the role passed Annual Certification until the next certification due date. No emails are sent to either users or Approvers in this case.
- Approvers are responsible for taking action to correct data in the trusted resource by the certification due date.

Users' Roles Removed – Approver Email Notification

- Approvers who are responsible for users who have validated role(s) will receive an email informing them of their users' role removal, when a validated role fails Annual Certification due to failing the validation check.
- A sample email is shown below.

From: <donotreply@cms.gov>
Date: Fri, Nov 20, 2015 at 4:29 PM
To:
Subject: Your CMS.gov users' roles have been removed.

The following Users', for whom you are listed as the Business Owner or Approver, have failed Annual Certification and their role(s) have been removed. The user details are attached.

Users who wish to regain access to their applications can request the role again by logging into CMS.gov using the link given below and requesting the desired role.

If you are accessing CMS.gov from CMS Net, Go to <CMS NET URL>.
If you are accessing CMS.gov from the Internet, Go to <Internet URL>.

Thank you,
CMS.gov
Please do not reply to this system generated E-mail.

Note:
Instructions for regaining access to the application are provided in the email.

Users' Roles Removed – User Email Notification

- Users with validated roles who failed Annual Certification will receive an email notifying the user of their role being removed.
- A sample email is shown below.

From: <donotreply@cms.gov>
Date: Fri, Nov 20, 2015 at 4:29 PM
To:
Subject: Your CMS.gov Application Role has been removed.

Dear <First Name> <Last Name>,

The Centers for Medicare and Medicaid Services (CMS) require that your Role, <Role Name>, in the <Application Name> Application be approved each year. This email is to notify you that your role has not been approved and has been removed.

If you wish to regain access to your application please request the role again by logging into CMS.gov using the link given below and requesting the desired role.

If you are accessing CMS.gov from CMS Net, Go to <CMS NET URL>.
If you are accessing CMS.gov from the Internet, Go to <Internet URL>.

If you need additional assistance contact your <Application Name> Help Desk at <Application Helpdesk email> or <Application Helpdesk phone number>.

Thank you,
CMS.gov
Please do not reply to this system generated E-mail.

Note:
Instructions for regaining access to the application are provided in the email.

Account Review

Account Review is the process of checking Users' accounts for the existence at least one (1) Application Role.

Some important terms related to Annual Certification and Account Reviews include:

- **Inactive** – The User has not logged into either their Application or EIDM for 60 days or more.
- **Locked** - The User is prevented from logging in to any application. They may login to EIDM. A User's account will be locked following 60 days of inactivity. To unlock an account, the User must login to EIDM, answer their challenge questions, and reset their password.
- **Deleted** – The User's account may no longer be used for any purpose and the User may register again. This occurs upon failing an Account Review when both statements below are true:
    - User's account does not have a Role in any Application and
    - User's account has been inactive for more than 360 days.

EIDM automatically performs calendar driven Account Reviews in March and October as shown in the chart below:

EIDM Checks performed (In order)	Result	Next Step/Action Taken
Does the account have a role?	Yes	Account review passes. No further action is taken.
	No	Proceed to the next step.
Has the account been inactive for less than 180 days?	Yes	Account review passes. No further action taken.
	No	Proceed to the next step.
Has the account been inactive for 180 days or more but less than 360 days?	Yes	Account Review fails. User is notified by Email.
	No	Proceed to the next step.
Has the account been inactive for 360 days or more?	Yes	Account Review fails. The account is deleted. The User is notified by Email and may re-register in EIDM.

Account Fails Review at 180 Days

- In the event an account fails review at 180 days, the account will be locked and an email will be sent to the user.
- A sample email is shown below.

From: <donotreply@cms.gov>
Date: Fri, Nov 20, 2015 at 4:29 PM
To:
Subject: Your CMS.gov Account has been locked.

Dear <First Name> <Last Name>,

The Centers for Medicare and Medicaid Services (CMS) periodically review CMS.gov User Accounts for compliance with CMS security policies.

Our records indicate that you do not have a role in any CMS.gov Application and you have not logged into CMS.gov for <number of days of inactivity> days or more. Due to this, your account, <User ID>, has been locked.

To unlock your Account, please login to CMS.gov using the link given below and follow the on-screen instructions.

If you are accessing CMS.gov from CMS Net, Go to <CMS NET URL>.
If you are accessing CMS.gov from the Internet, Go to <Internet URL>.

Thank you,
CMS.gov
Please do not reply to this system generated E-mail.

Note:
Locked users can unlock using the self-service function by answering the challenge questions that they setup at the time of registration and resetting their password.

Account Fails Review at 360 Days

- In the event that an account fails review at 360 days, the account will be deleted and an email will be sent to the user.
- A sample email is shown below.
-

From: <donotreply@cms.gov>
Date: Fri, Nov 20, 2015 at 4:29 PM
To:
Subject: Your CMS.gov Account has been deleted.

Dear <First Name> <Last Name>,

The Centers for Medicare and Medicaid Services (CMS) periodically review CMS.gov User Accounts for compliance with CMS security policies.

Our records indicate that you do not have a role in any CMS.gov Application and you have not logged into CMS.gov for <number of days of inactivity> days or more. Due to this, your account, <User ID>, has been deleted.

To regain access to CMS.gov and it's Applications you may register for a new Account by accessing CMS.gov using the link given below and selecting the New User Registration link.

If you are accessing CMS.gov from CMS Net, Go to <CMS NET URL>.
If you are accessing CMS.gov from the Internet, Go to <Internet URL>.

Thank you,
CMS.gov
Please do not reply to this system generated E-mail.

Note:
The email will include instructions to regain access to CMS.gov by registering for a new user account.

5. Manage Users

This section provides the following:

- How to search for a user.
- How to remove a role attribute.
- How to remove a role.
- How to remove multiple roles or attributes.
- How to use the Export Result feature.

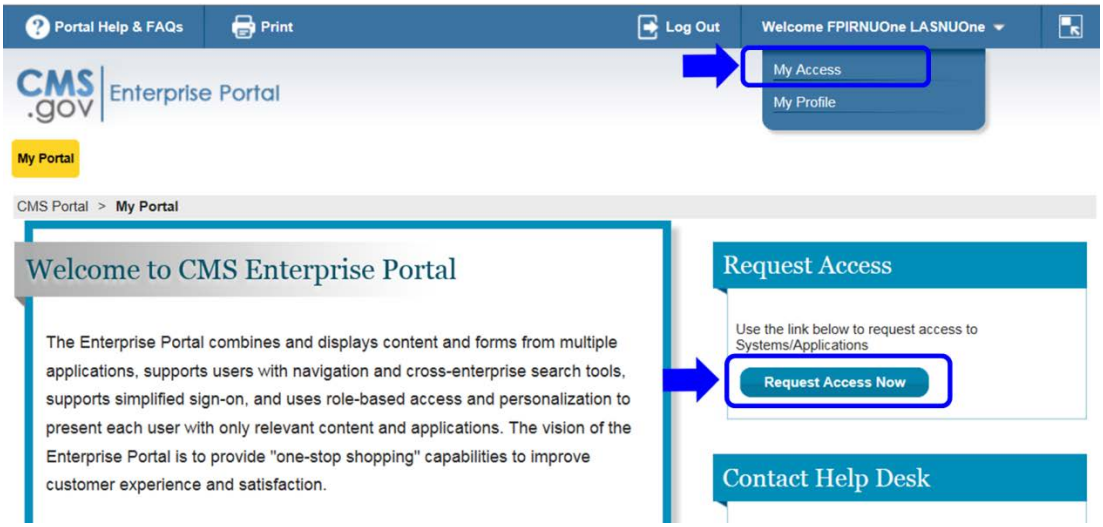
How to search for a user

The following are the basic step-by-step instructions on how to use the **Application Search** via **View and Manage Users**. The **Application Search** feature allows Application Approvers to search and manage the accounts of users who are under their authority.

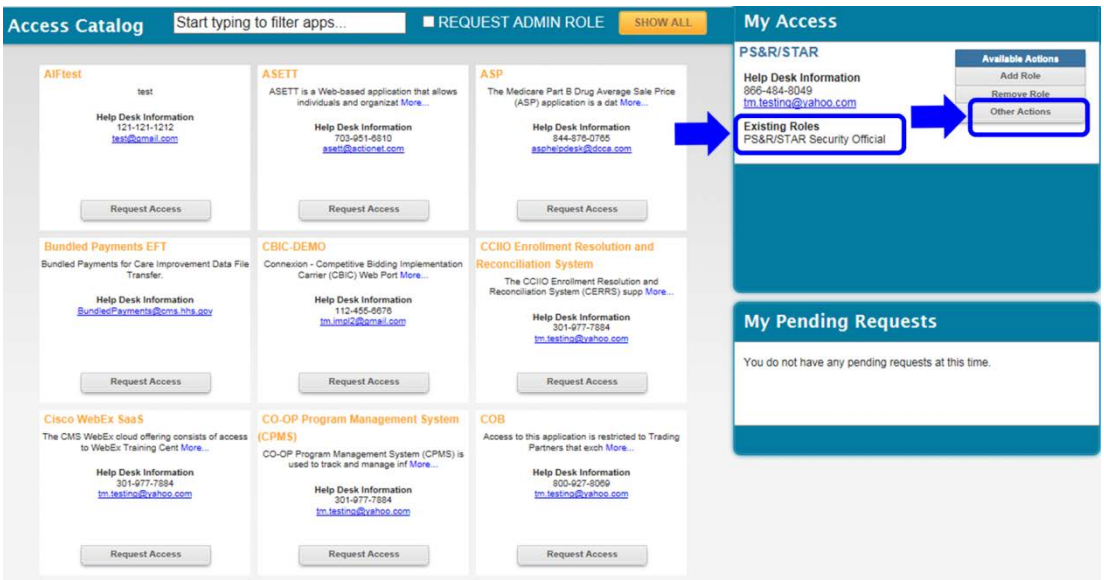
	Action
Step 1	After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed. Select the down arrow icon that appears next to your name at the top of page. Then, select **My Access** from the drop down menu to continue. Alternately, you may select **Request Access Now** to continue.

Note:

After logging in, EIDM will check to see if you are an approver for one or more applications.



Action	
Step 2	The **Access Catalog**, **My Access** and **My Pending Requests** sections are displayed. The existing roles you have in each application are displayed in the **My Access** section. Select **Other Actions** in the **My Access** section to continue. If there are multiple **Other Actions** options displayed, you may select any "Other Actions" option to continue.



Step 3	The **View and Manage My Access** page is displayed. Select **View and Manage Users** to continue.

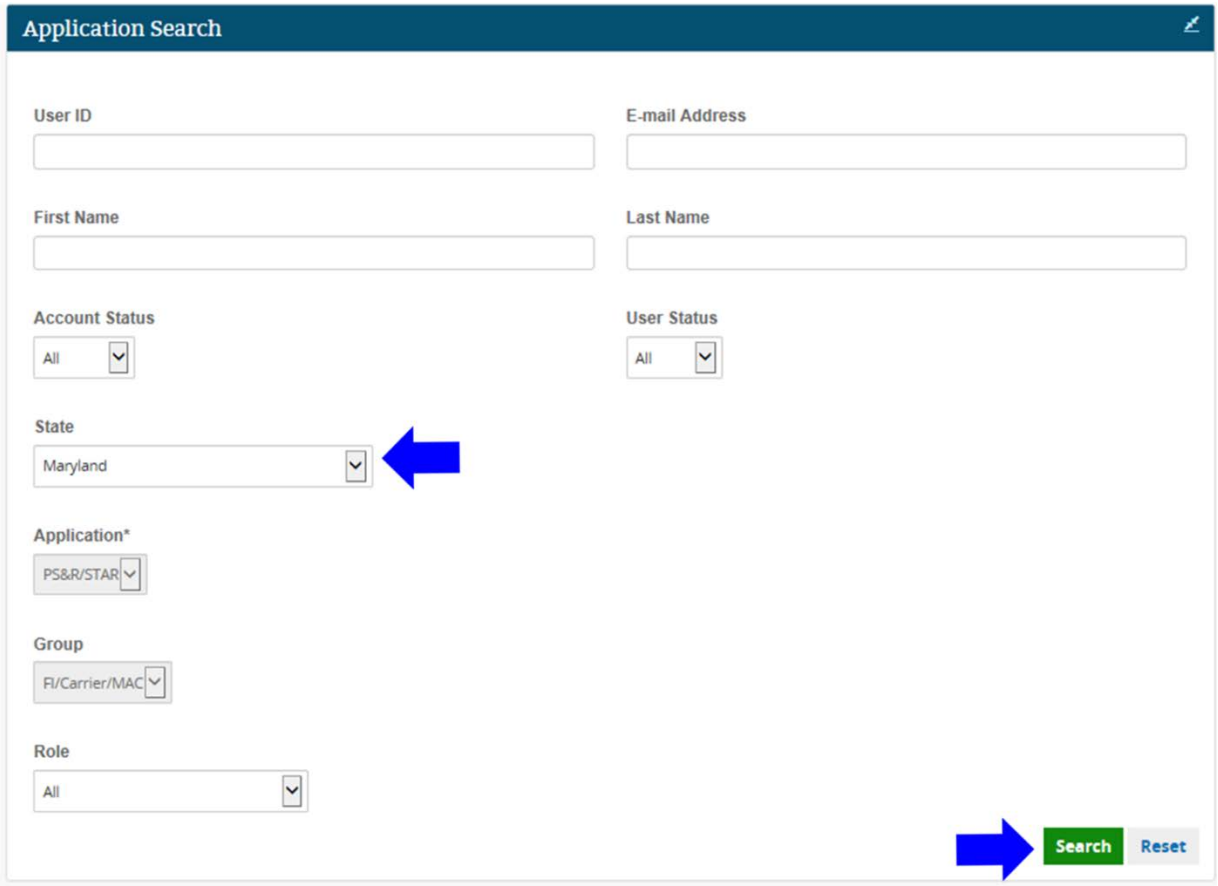
Step 4	The **Application Search** page is displayed. You may search for an individual, or individuals, by entering at least the Application as the search criteria or a combination of Application and any of the options such as, User ID, First Name, Last Name, E-mail address, User Status, Account Status, State, Role and Role Attributes. A Minimum of two (2) characters must be entered if user ID, First Name, Last

Action

Name, or E-mail are used for the search criteria.

Provide the appropriate information to locate the individual or individuals needed and then select **Search**.

The example below shows a search for users in the state of Maryland.



Step 5 After selecting **Search**, all of the users in the application matching the search criteria, that you are authorized to view, are displayed in the **Search Results** section.

Select the person's **User ID** to view the user's details.

Note:

You may select **Cancel** at any time to exit out of the View and Manage Users process. Any search information, user information or changes entered will not be saved.

Action

Application Search

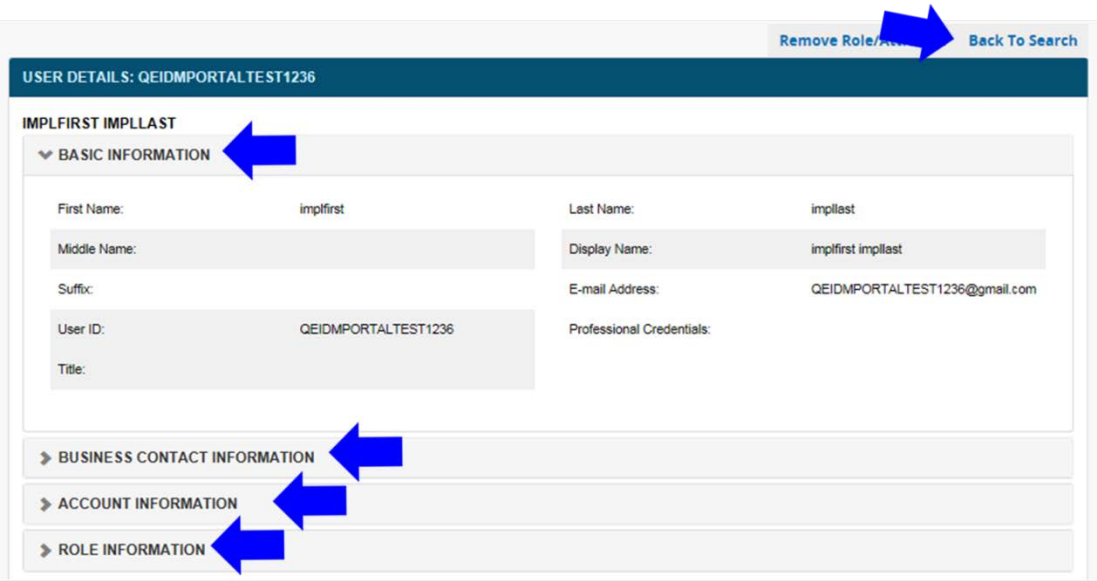
Showing 1 to 11 of 11 matching records in PS&R/STAR

Sort By User ID In Ascending Sort Export Results

User ID	User Details	Status	Role	Actions
QEIDMPORTALTEST1238	: implfirst impllast **Email:** srahi77@yahoo.com **State:** MD	**Account:** Unlocked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 11	
QEIDMPORTALTEST1227	**Name:** implfirst impllast **Email:** rmangal@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** PS&R Admin	
QEIDMPORTALTEST1228	**Name:** implfirst impllast **Email:** mnazir@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** PS&R User	
QEIDMPORTALTEST1230	**Name:** implfirst impllast **Email:** rtester786@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 8	
QEIDMPORTALTEST1231	**Name:** implfirst impllast **Email:** spadala_con@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 3	
QEIDMPORTALTEST1232	**Name:** implfirst impllast **Email:** azeltser@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 4	
QEIDMPORTALTEST1233	**Name:** implfirst impllast **Email:** QEIDMPORTALTEST1233@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 5	
QEIDMPORTALTEST1234	**Name:** implfirst impllast **Email:** QEIDMPORTALTEST1234@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 6	
QEIDMPORTALTEST1235	**Name:** implfirst impllast **Email:** QEIDMPORTALTEST1235@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 7	
QEIDMPORTALTEST1236	**Name:** implfirst impllast **Email:** QEIDMPORTALTEST1236@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 2	
QEIDMPORTALTEST1237	**Name:** implfirst impllast **Email:** QEIDMPORTALTEST1237@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 10	

Results Per Page First Previous Next Last Showing Page 1 Of 1

	Action
Step 6	The **User Details** page is displayed. The page displays **Basic Information**, **Business Contact Information**, **Account Information** and **Role Information** about the user. Expand each arrow to view the details. Select **Back To Search** to close the User Details page and return to the Application Search.



Action

How to remove a role attribute

This section shows how to remove role attribute from a user's profile, if you have the authority. See **Section 7: Approver Roles and Functions** for approver roles and the functions they are authorized to perform.

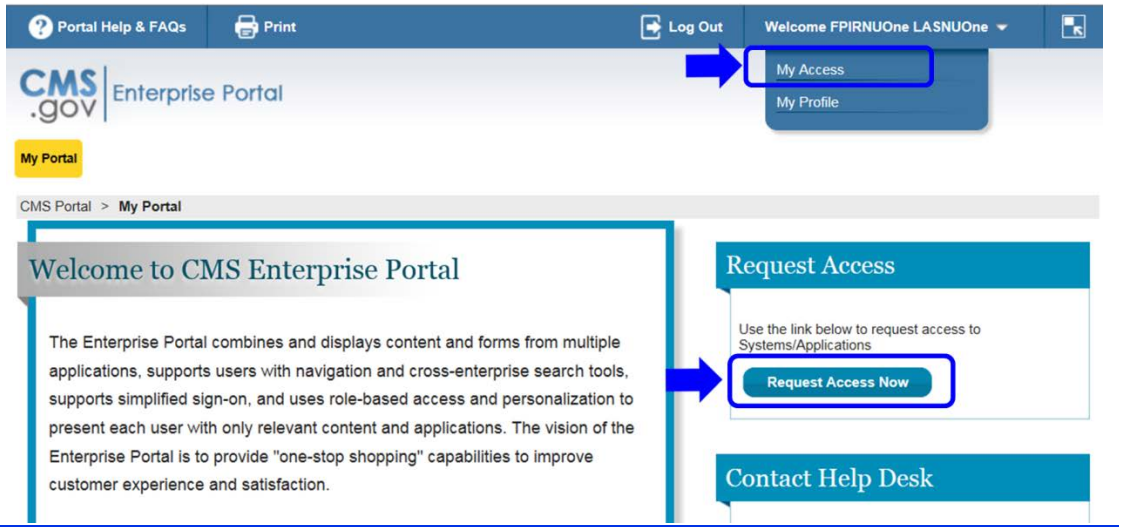
You must select a role in the search criteria for the 'Remove Roles/Attributes' option to be available on the results page.

The following are the basic step-by-step instructions on how to use the **View and Manage Users** feature to remove a role attribute.

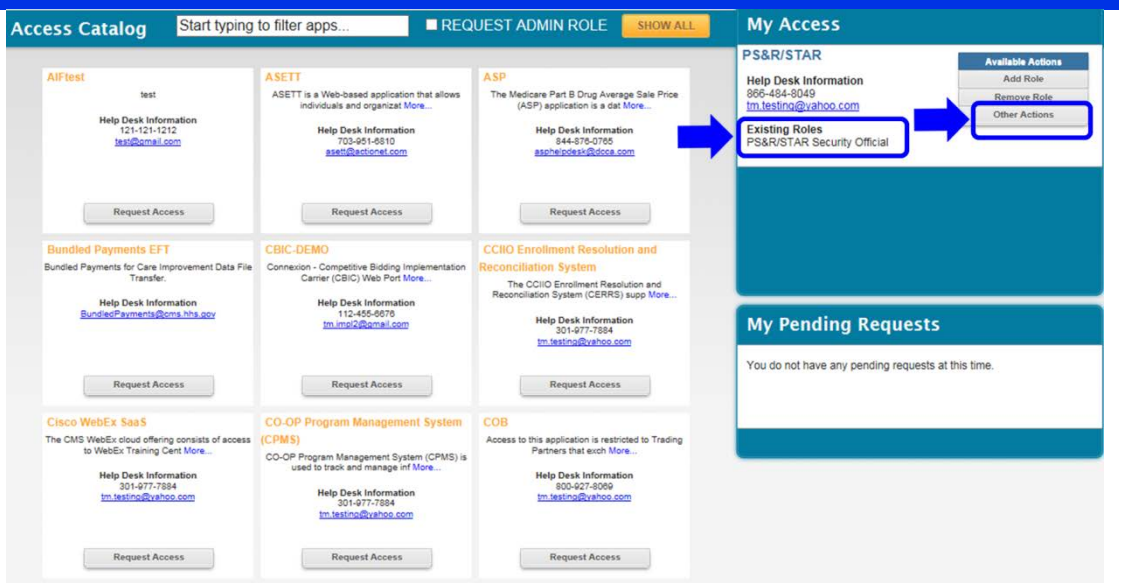
	Action
Step 1	After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed. Select the down arrow icon that appears next to your name at the top of page. Then, select **My Access** from the drop down menu to continue. Alternately, you may select **Request Access Now** to continue.

Note:

After logging in, EIDM will check to see if you are an approver for one or more applications.



Step 2	The **Access Catalog**, **My Access** and **My Pending Requests** sections are displayed. The existing roles you have in each application are displayed in the **My Access** section. Select **Other Actions** in the **My Access** section to continue. If there are multiple **Other Actions** options displayed, you may select any “Other Actions” option to continue.

Action


Step 3 The **View and Manage My Access** page is displayed.

Select **View and Manage Users** to continue.

Step 4 The **Application Search** page is displayed.

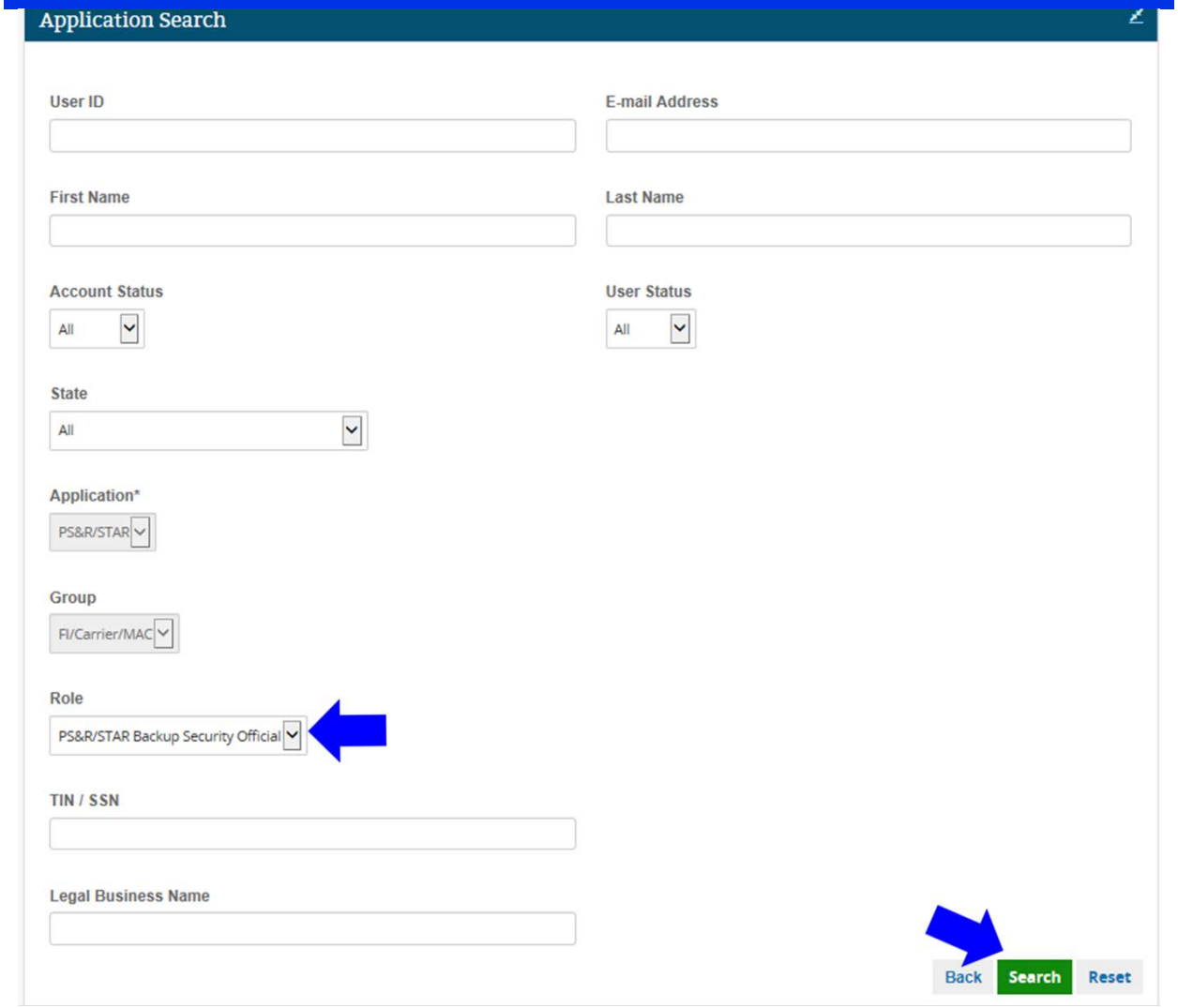
You may search for an individual, or individuals, by entering at least the Application as the search criteria or a combination of Application and any of the options such as, User ID, First Name, Last Name, E-mail Address, User Status, Account Status, State, Role and Role Attributes.

A Minimum of two (2) characters must be entered if User ID, First Name, Last Name, or E-mail Address is used for the search criteria.

You must select a role in the search criteria for the 'Remove Roles/Attributes' option to be available on the results page**.**

Provide the appropriate information to locate the individual or individuals needed and then select **Search**.

Action



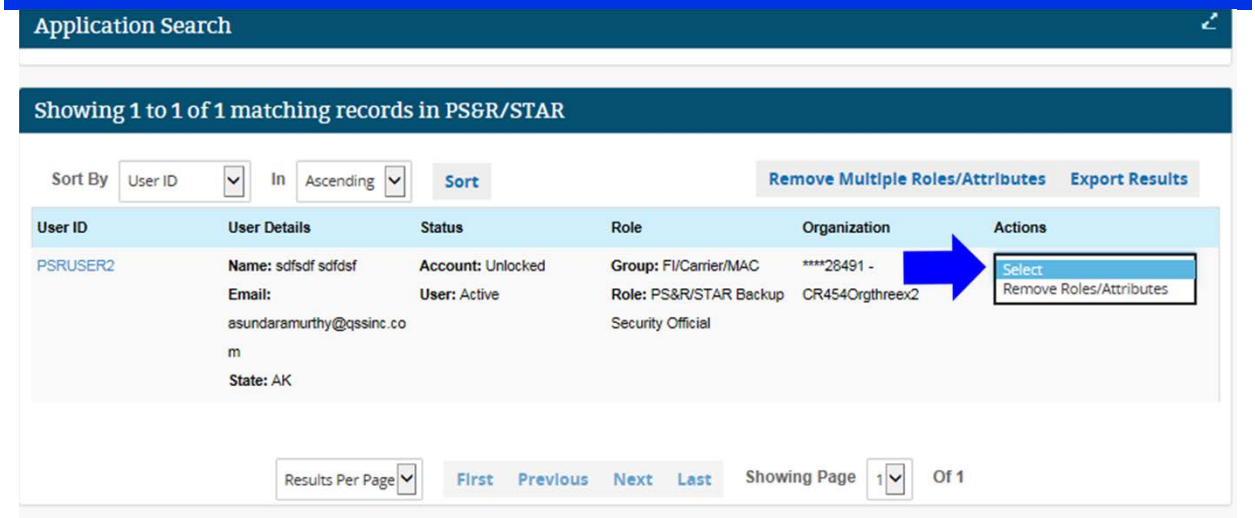
Step 5 After selecting **Search**, all of the persons in the application matching the search criteria, that you are authorized to view, are displayed in the **Search Results** section.

Under **Actions**, select **Remove Roles/Attributes** from the drop down menu.

Note:

You may select **Cancel** at any time to exit out of the View and Manage Users process. Any search information, user information or changes entered will not be saved.

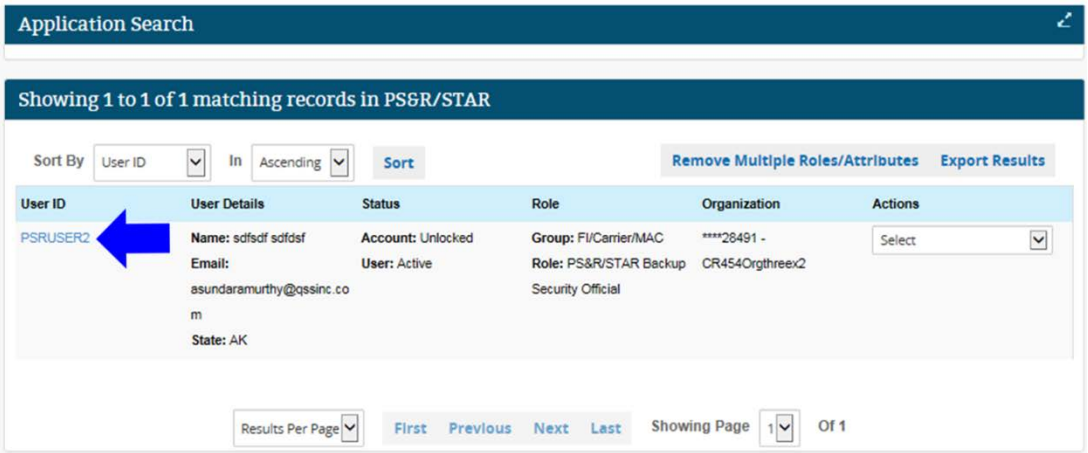
Action



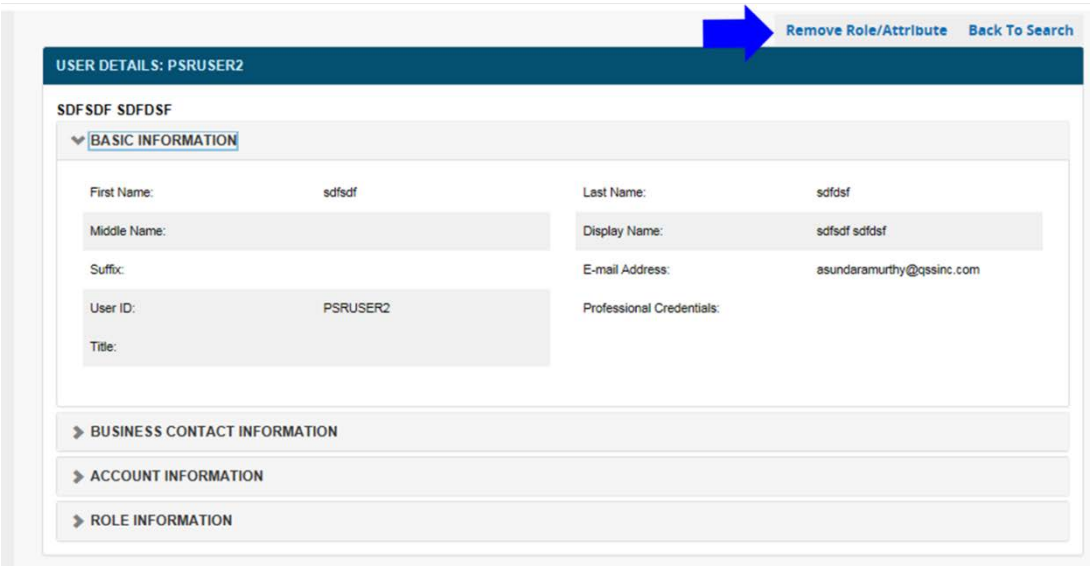
Step 6 Alternately, select the person's **User ID** to view the person's role information.

The **User Details** page is displayed.

Select **Remove Role/Attribute** at the top of the page.



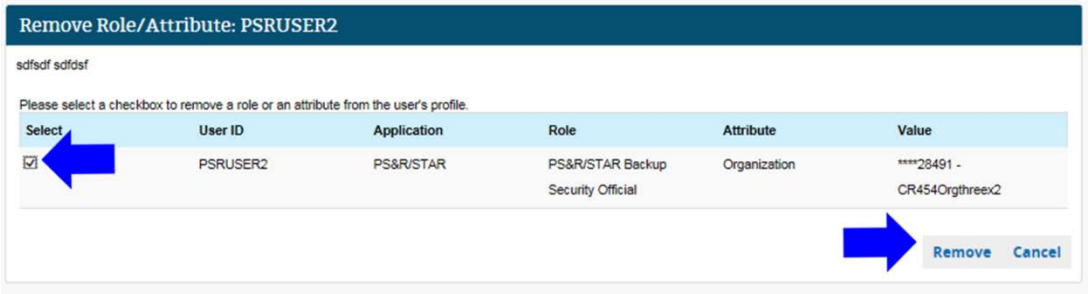
Action



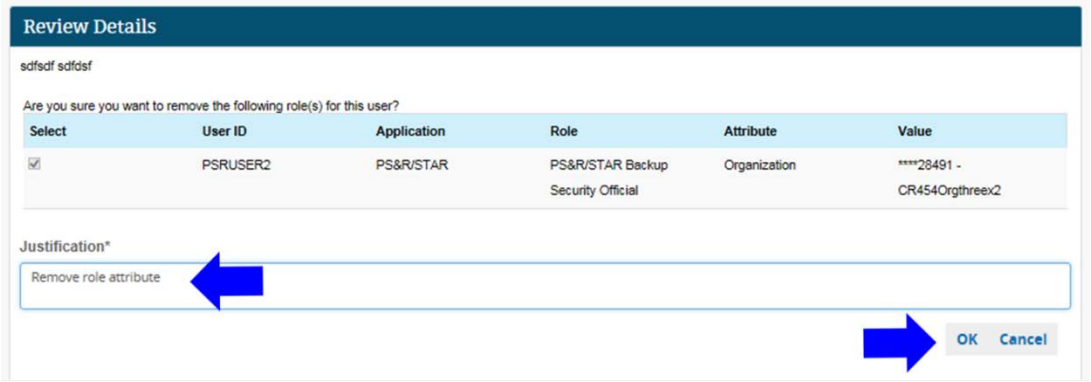
Step 7 The **RemoveRole/Attribute** page is displayed.

Select the check box next to the attribute to be removed.

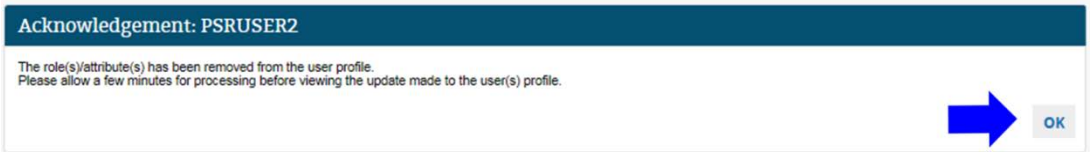
Select **Remove** to remove the attribute.



Step 8 Enter a justification for the role attribute removal and select **OK**.



Action	
Step 9	You will receive an acknowledgement message. Select **OK** to return to the **Application Search** page.



How to remove a role

This section shows how to remove a call center from a person's role, if you have the authority. See **Section 7: Approver Roles and Functions** for approver roles and the functions they are authorized to perform.

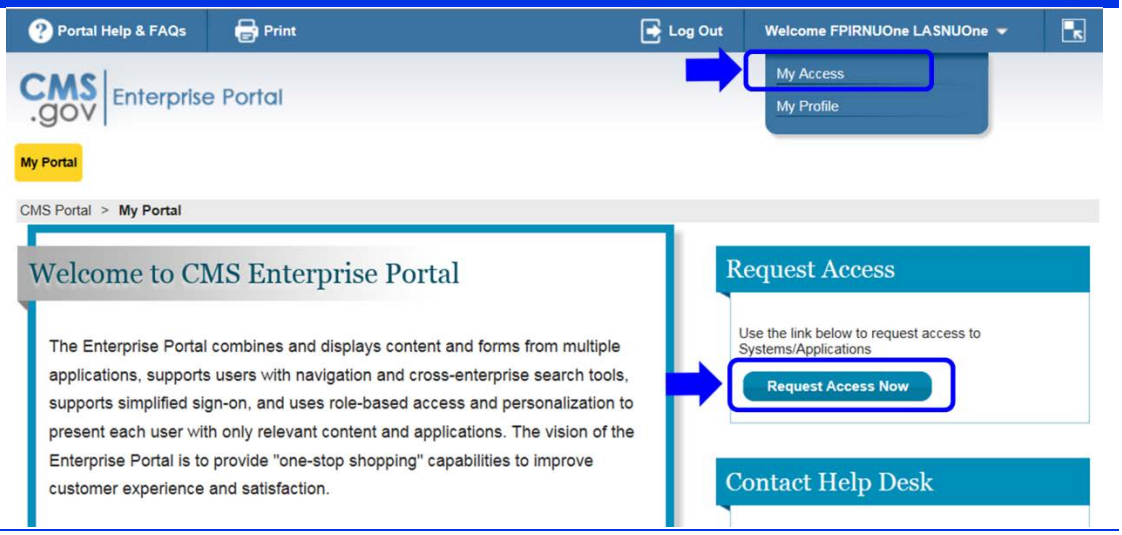
You must select a role in the search criteria for the 'Remove Roles/Attributes' option to be available on the results page**.**

The following are the basic step-by-step instructions on how to use the **View and Manage Users** feature to remove a call center.

Action	
Step 1	After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed. Select the down arrow icon that appears next to your name at the top of page. Then, select **My Access** from the drop down menu to continue.

Alternately, you may select Request Access Now to continue. Note:
After logging in, EIDM will check to see if you are an approver for one or more applications.

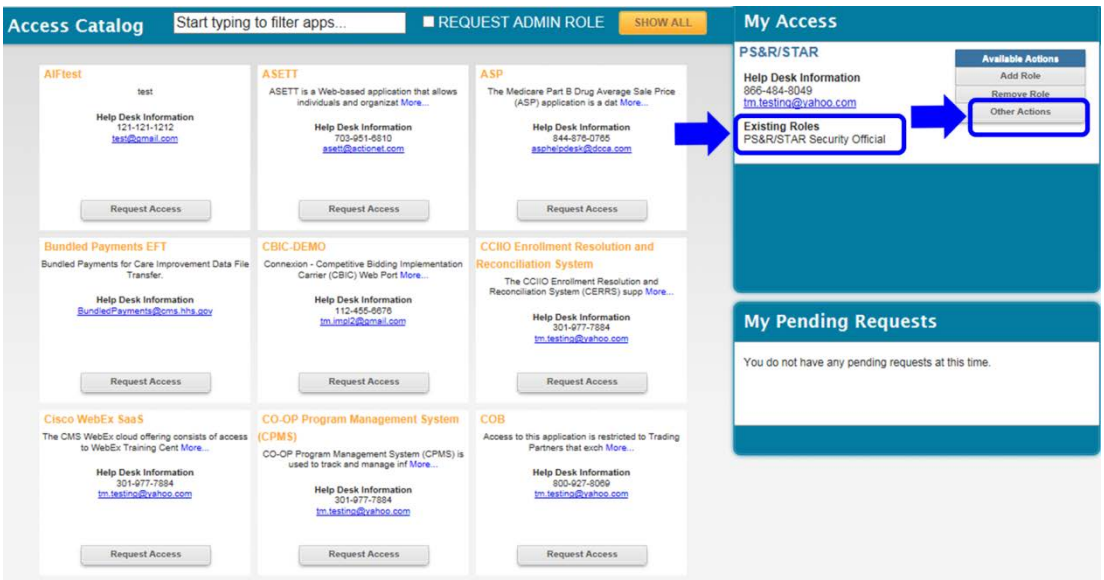
Action



Step 2 The **Access Catalog**, **My Access** and **My Pending Requests** sections are displayed.

The existing roles you have in each application are displayed in the **My Access** section.

Select **Other Actions** in the **My Access** section to continue. If there are multiple **Other Actions** options displayed, you may select any "Other Actions" option to continue.



Step 3 The **View and Manage My Access** page is displayed.
Select **View and Manage Users** to continue.

Action

Step 4 The **Application Search** page is displayed.

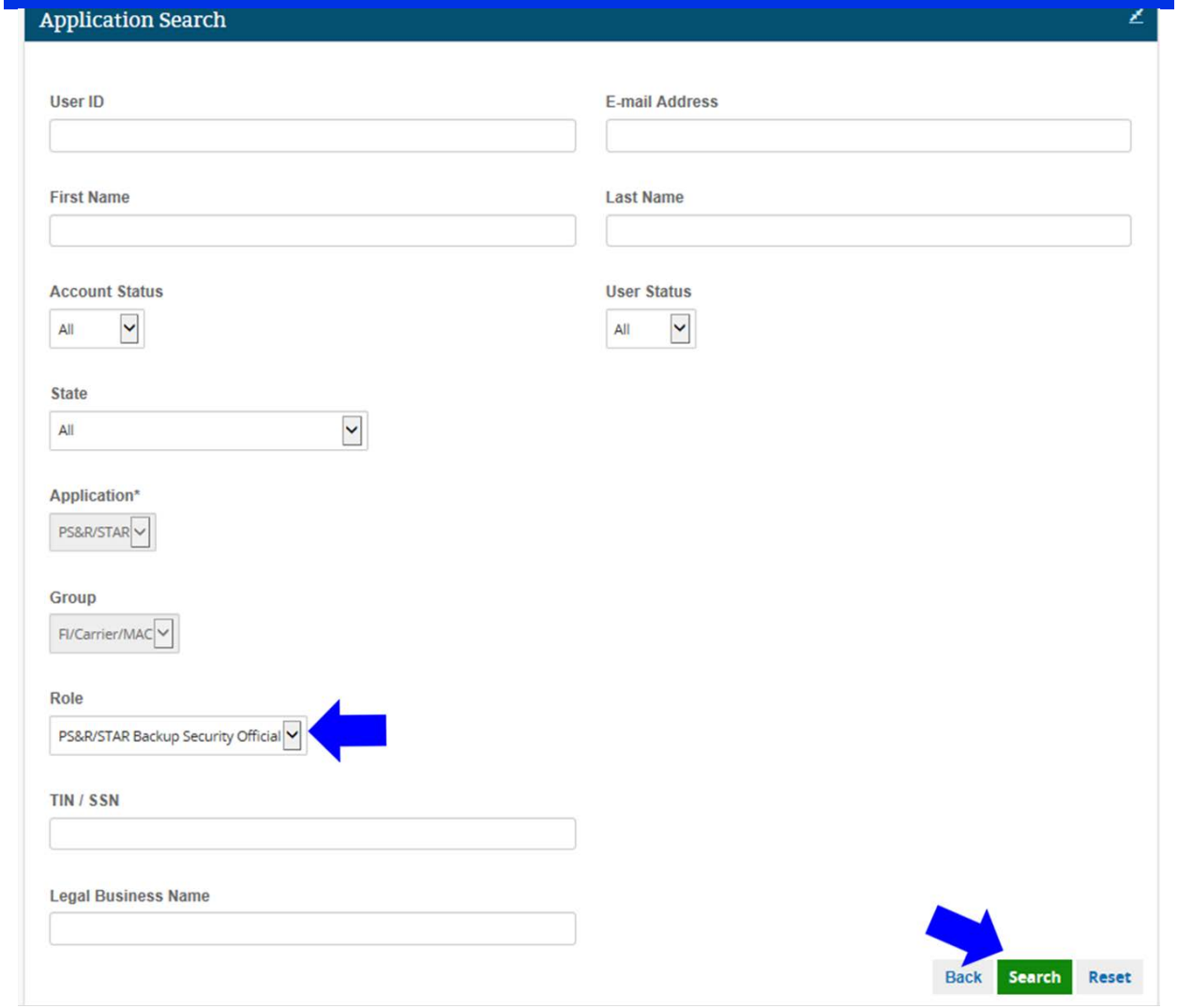
You may search for an individual, or individuals, by entering at least the Application as the search criteria or a combination of Application and any of the options such as, User ID, First Name, Last Name, E-mail address, User Status, Account Status, State, Role and Role Attributes.

A Minimum of two (2) characters must be entered if user ID, First Name, Last Name, or E-mail are used for the search criteria.

You must select a role in the search criteria for the 'Remove Roles/Attributes' option to be available on the results page**.**

Provide the appropriate information to locate the individual or individuals needed and then select **Search**.

Action



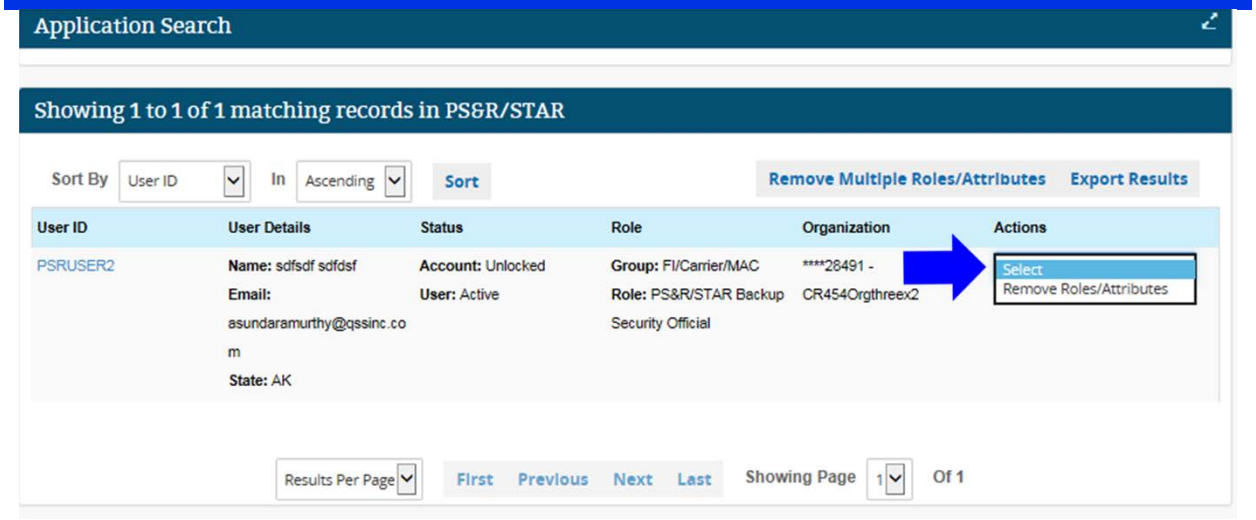
Step 5 After selecting **Search**, all of the persons in the application matching the search criteria, that you are authorized to view, are displayed in the **Search Results** section.

Under **Actions**, select **Remove Roles/Attributes** from the drop down menu.

Note:

You may select **Cancel** at any time to exit out of the View and Manage Users process. Any search information, user information or changes entered will not be saved.

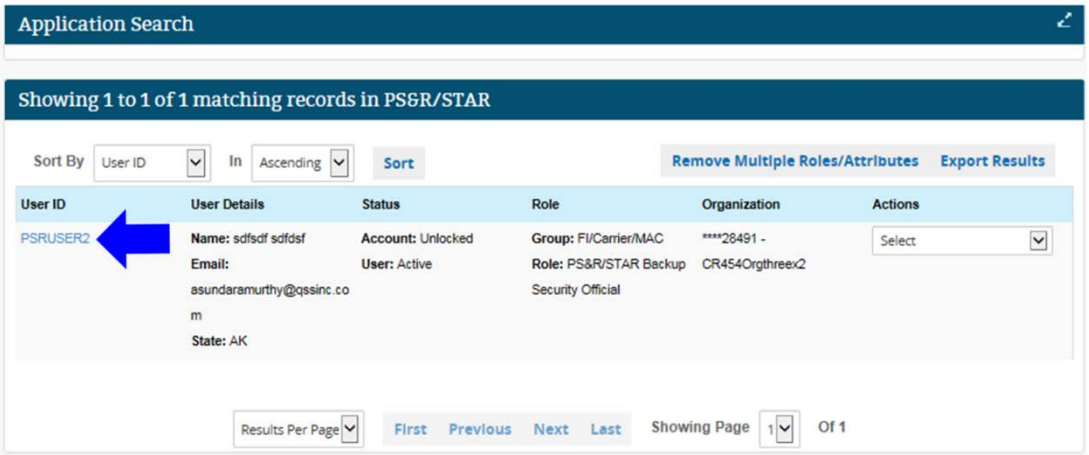
Action



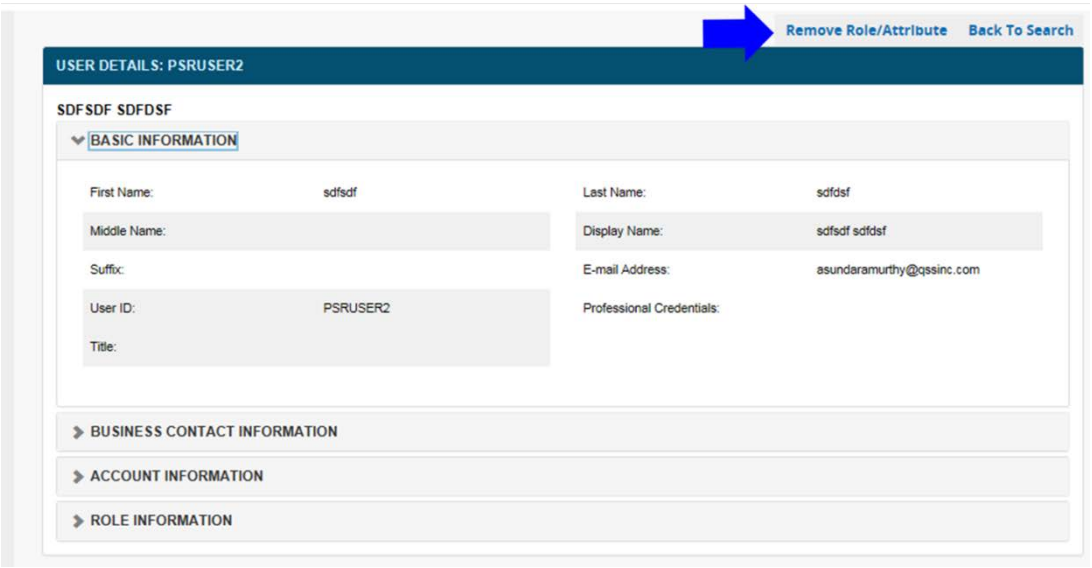
Step 6 Alternately, select the person's **User ID** to view the person's role information.

The **User Details** page is displayed.

Select **Remove Role/Attribute** at the top of the page.



Action



Step 7 The **RemoveRole/Attribute** page is displayed.

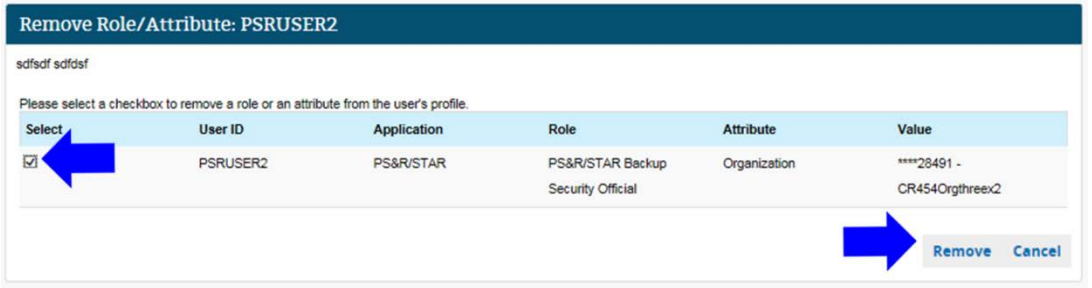
In the example below the user has only one role with one attribute.

Select the check for the role to be removed.

Select **Remove** to remove the role and the associated attributes.

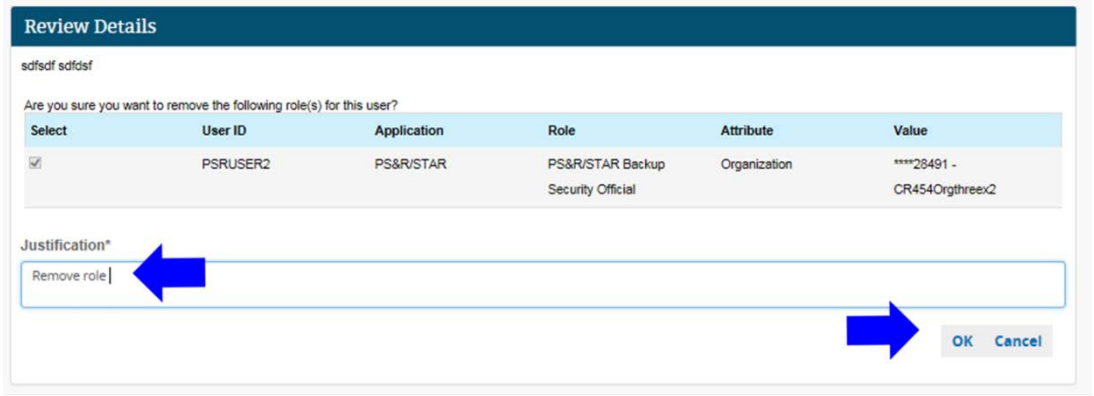
Note:

Select the checkbox for all the attributes associated to a role in order to remove a role from the user's profile.



Step 8 Enter a justification for the role removal and select **OK**.

Action



Step 9 You will receive an acknowledgement message.

Select **OK** to return to the **Application Search** page.

How to remove multiple roles or attributes

The following are the basic step-by-step instructions on how to use the **View and Manage Users** feature to remove one or more roles or attributes from one or more users, if you have the authority.

You must select a role in the search criteria for the 'Remove Multiple Roles/Attributes' button to be available on the results page**.**

Action

Step 1 After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed.

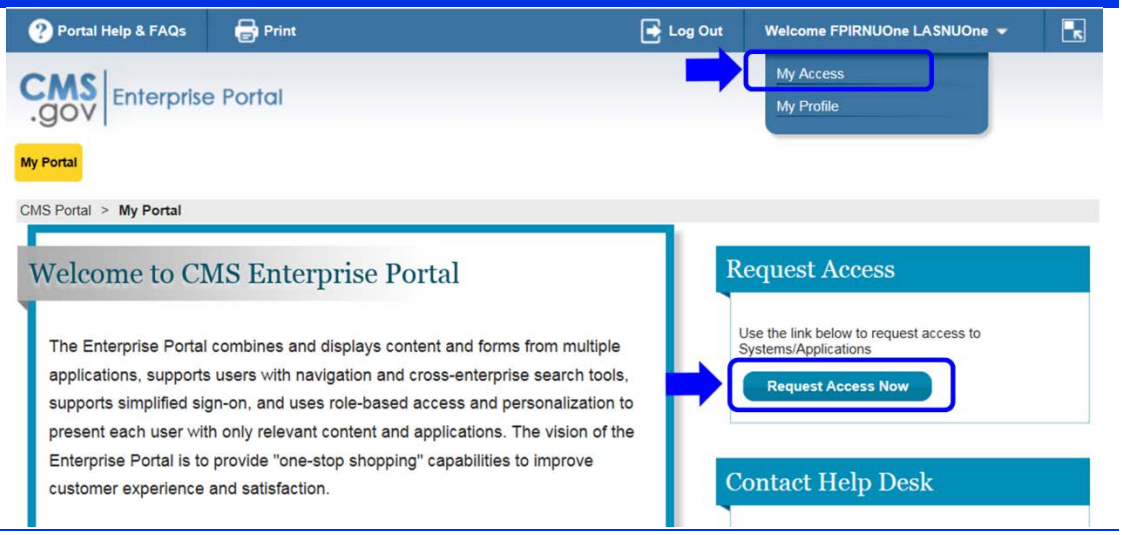
Select the down arrow icon that appears next to your name at the top of page. Then, select **My Access** from the drop down menu to continue.

Alternately, you may select **Request Access Now** to continue.

Note:

After logging in, EIDM will check to see if you are an approver for one or more applications.

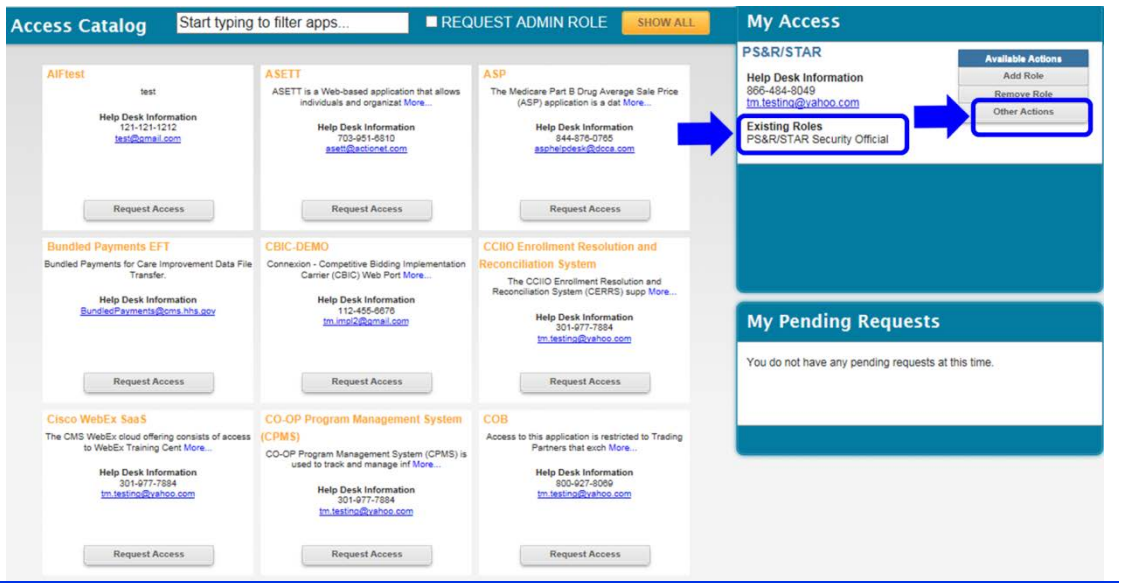
Action



Step 2 The **Access Catalog**, **My Access** and **My Pending Requests** sections are displayed.

Any existing roles you have in each application are displayed in the **My Access** section.

Select **Other Actions** in the **My Access** section to continue. If there are multiple **Other Actions** options displayed, you may select any "Other Actions" option to continue.



Step 3 The **View and Manage My Access** page is displayed.

Select View and Manage Users to continue.

Action

Step 4 The **Application Search** page is displayed.

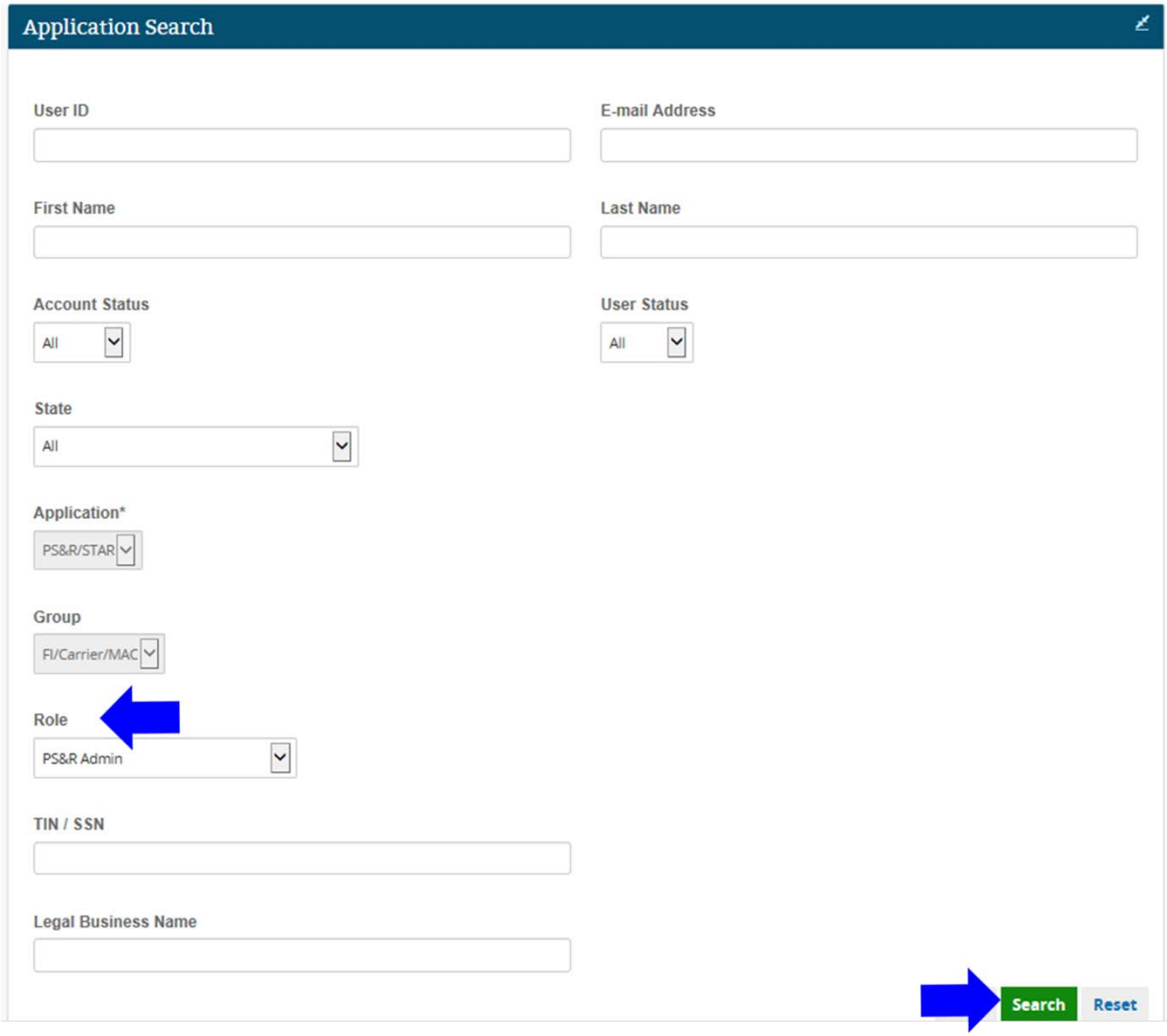
You may search for an individual, or individuals, by entering at least the Application as the search criteria or a combination of Application and any of the options such as, User ID, First Name, Last Name, E-mail address, User Status, Account Status, State, Role and Role Attributes.

A Minimum of two (2) characters must be entered if user ID, First Name, Last Name, or E-mail are used for the search criteria.

You must select a role in the search criteria for the 'Remove Multiple Roles/Attributes' button to be available on the results page**.**

Provide the appropriate information to locate the individual or individuals needed and then select **Search**.

Action



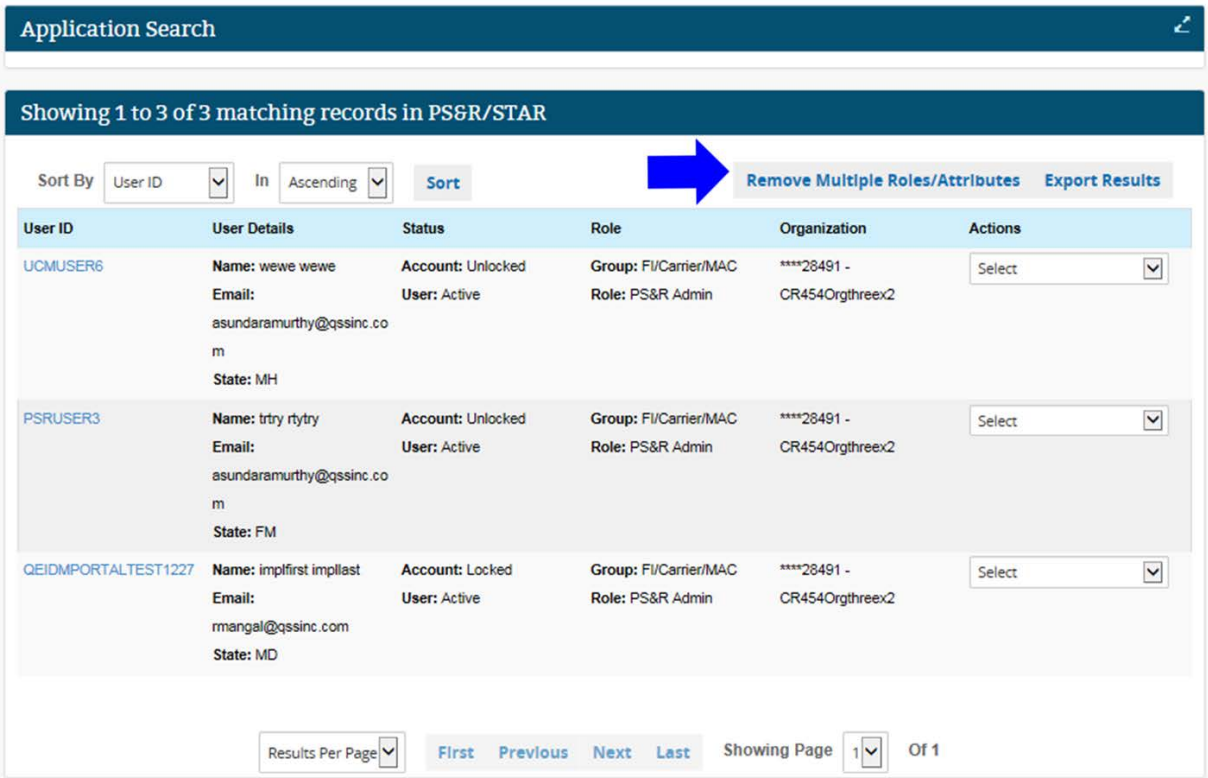
Step 5 After selecting **Search**, all of the persons in the application matching the search criteria, that you are authorized to view, are displayed in the **Search Results** section.

Select the **Remove Multiple Roles/Attributes** option.

Note:

You may select **Cancel** at any time to exit out of the View and Manage Users process. Any search information, user information or changes entered will not be saved.

Action



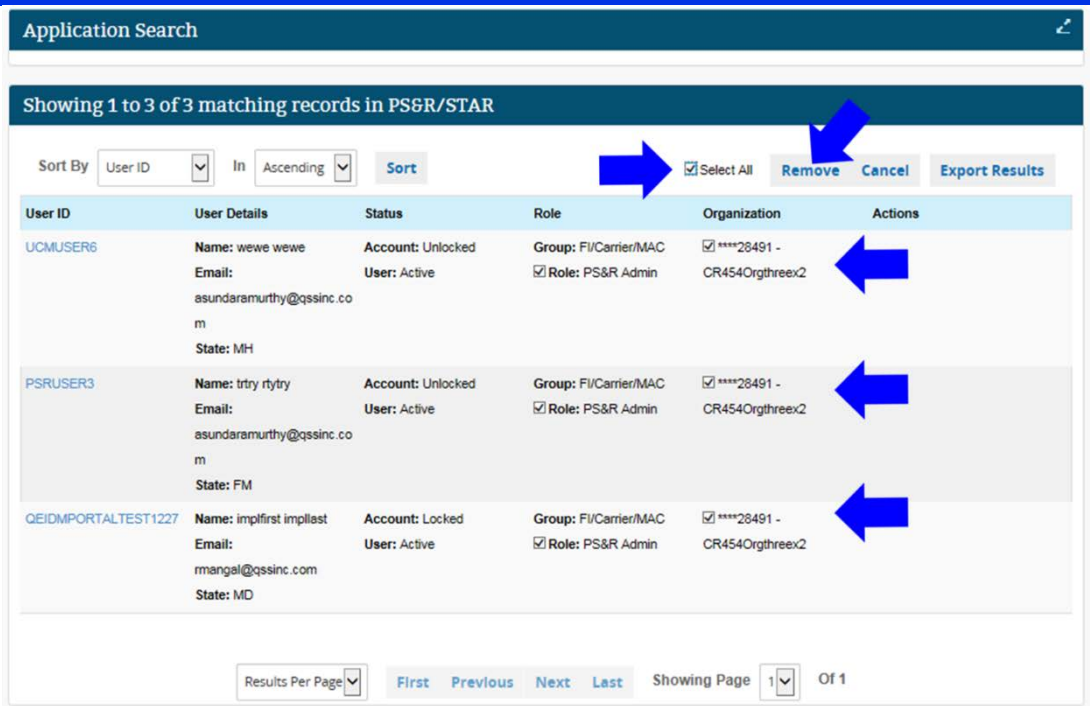
Step 6 The page updates to include checkboxes beside all roles and attributes and displays the 'Select All' checkbox, 'Remove' button, and 'Cancel' button.

Check the boxes for the roles/attributes you want to remove and select **Remove**.

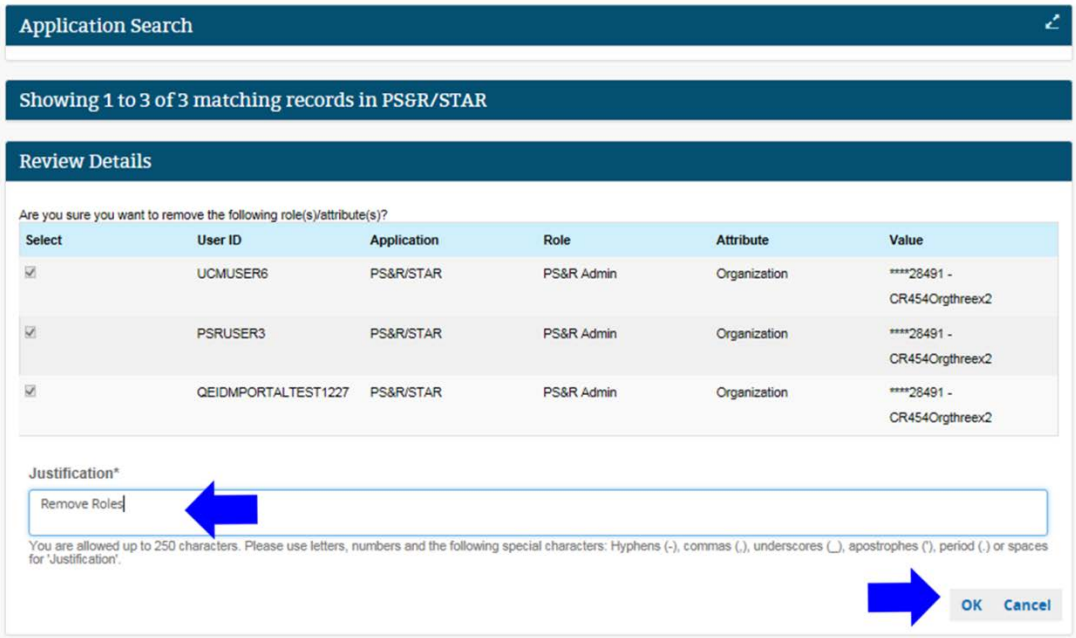
You may also **Select All** to select all the roles or attributes that you wish to remove on the page.

Select **Remove** to remove the roles selected.

Action



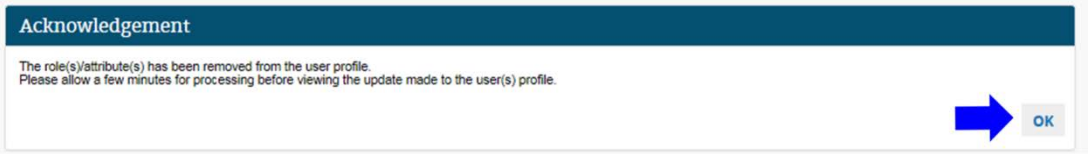
Step 7 Enter a justification for the role removal and select **OK**.



Step 8 You will receive an acknowledgement message.

Select **OK** to return to the **Application Search** page.

Action



How to use the Export Results feature

The following are the basic step-by-step instructions on how to use the **Export Results** feature to export search result to an Excel spreadsheet.

Action

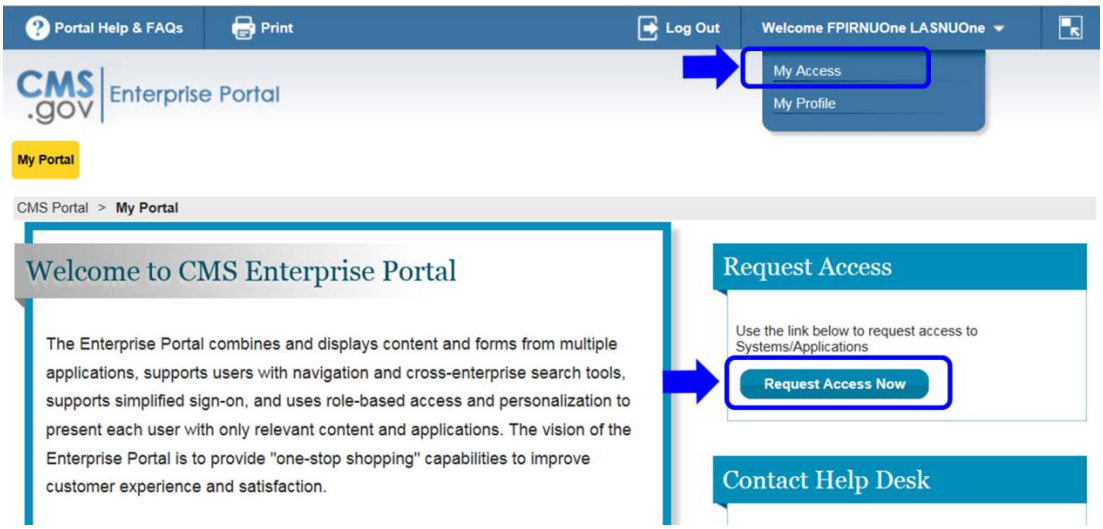
Step 1 After navigating to the **CMS Enterprise Portal** (https://portal.cms.gov), accepting the **Terms and Conditions**, and logging in with your User ID and password, the **Welcome to CMS Enterprise Portal** page is displayed.

Select the down arrow icon that appears next to your name at the top of page. Then, select **My Access** from the drop down menu to continue.

Alternately, you may select **Request Access Now** to continue.

Note:

After logging in, EIDM will check to see if you are an approver for one or more applications.

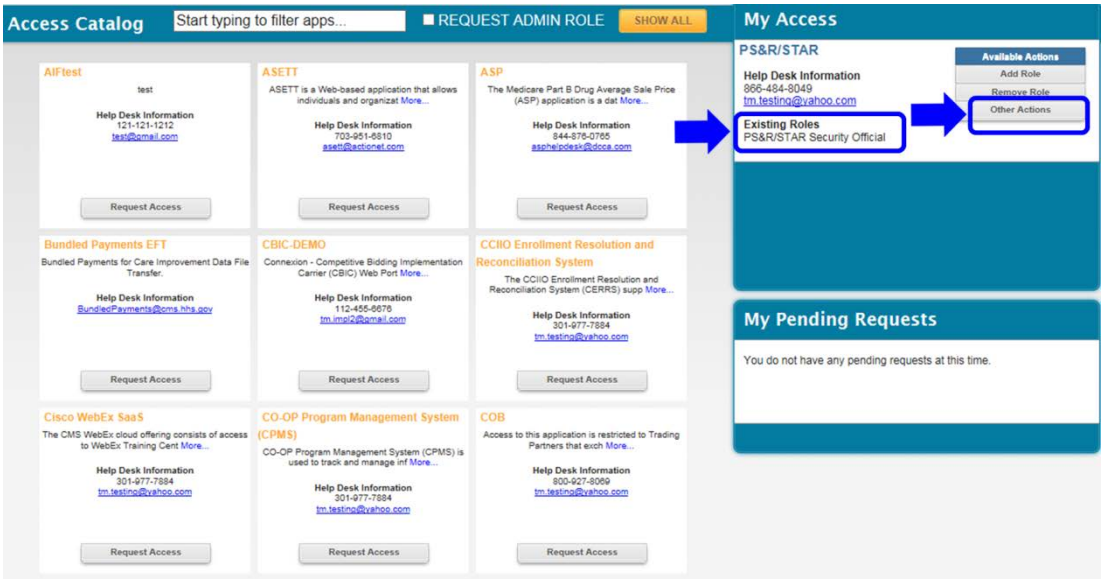


Step 2 The **Access Catalog**, **My Access** and **My Pending Requests** sections are displayed.

Any existing roles you have in each application are displayed in the **My Access** section.

Select **Other Actions** in the **My Access** section to continue.

Action



Step 3 The **View and Manage My Access** page is displayed.

Select **View and Manage Users** to continue.

Step 4 The **Application Search** page is displayed.

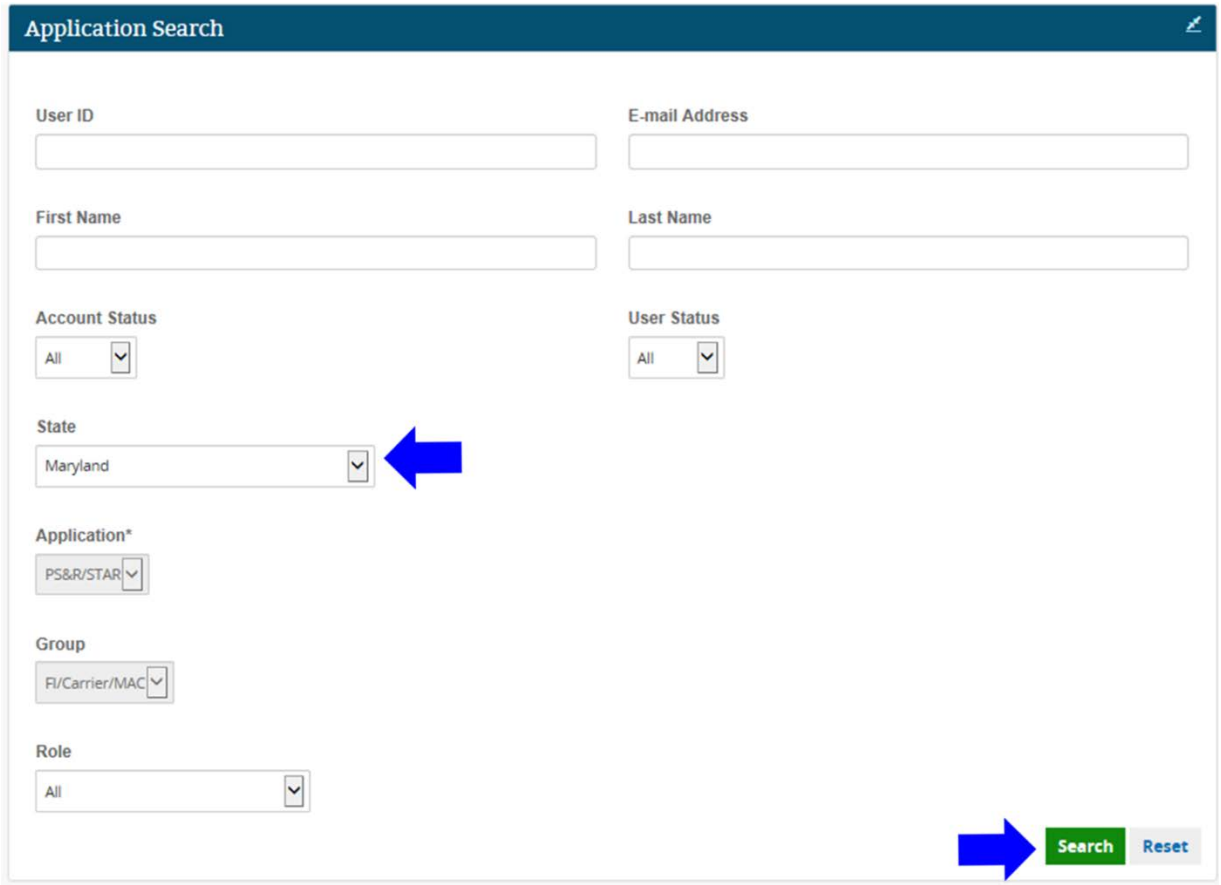
You may search for an individual, or individuals, by entering at least the Application as the search criteria or a combination of Application and any of the options such as, User ID, First Name, Last Name, E-mail address, User Status, Account Status, State, Role and Role Attributes.

A Minimum of two (2) characters must be entered if user ID, First Name, Last Name, or E-mail are used for the search criteria.

Provide the appropriate information to locate the individual or individuals needed and then select **Search**.

The example below shows a search for users in the state of Maryland.

Action



Step 5 After selecting **Search**, all of the users in the application matching the search criteria, that you are authorized to view, are displayed in the **Search Results** section.

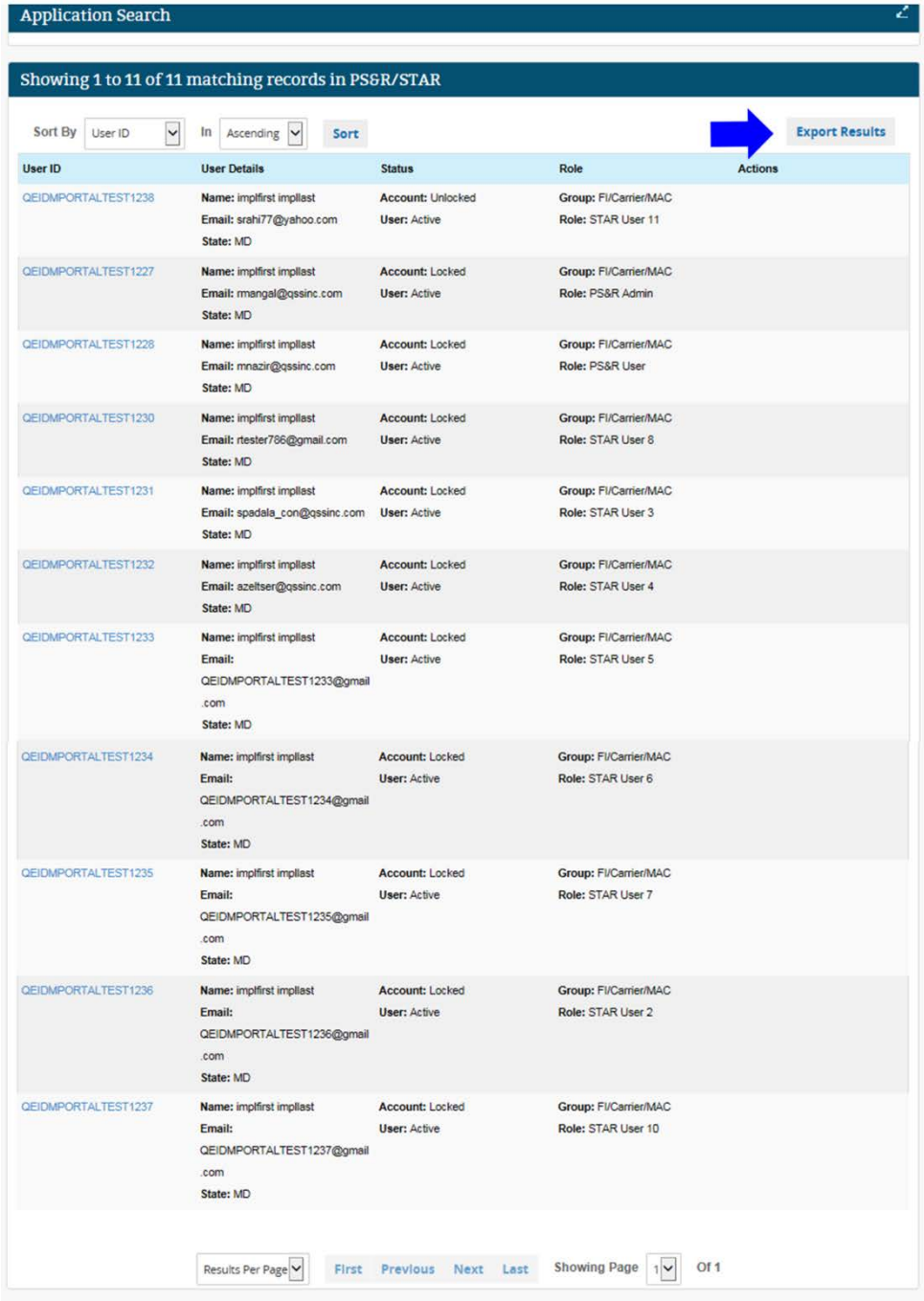
Select the **Export Results** button. The results of the search will be exported to an Excel spreadsheet.

Note:

The Export Results limit for the Application Search is 1000 users.

You may select **Cancel** at any time to exit out of the View and Manage Users process. Search information, user information or changes entered will not be saved.

Action



Application Search

Showing 1 to 11 of 11 matching records in PS&R/STAR

Sort By User ID In Ascending Sort

Export Results

User ID	User Details	Status	Role	Actions
QEIDMPORTALTEST1238	**Name:** implfirst implllast **Email:** srahi77@yahoo.com **State:** MD	**Account:** Unlocked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 11	
QEIDMPORTALTEST1227	**Name:** implfirst implllast **Email:** rmangal@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** PS&R Admin	
QEIDMPORTALTEST1228	**Name:** implfirst implllast **Email:** mnazir@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** PS&R User	
QEIDMPORTALTEST1230	**Name:** implfirst implllast **Email:** rtester786@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 8	
QEIDMPORTALTEST1231	**Name:** implfirst implllast **Email:** spadala_con@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 3	
QEIDMPORTALTEST1232	**Name:** implfirst implllast **Email:** azeltser@qssinc.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 4	
QEIDMPORTALTEST1233	**Name:** implfirst implllast **Email:** QEIDMPORTALTEST1233@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 5	
QEIDMPORTALTEST1234	**Name:** implfirst implllast **Email:** QEIDMPORTALTEST1234@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 6	
QEIDMPORTALTEST1235	**Name:** implfirst implllast **Email:** QEIDMPORTALTEST1235@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 7	
QEIDMPORTALTEST1236	**Name:** implfirst implllast **Email:** QEIDMPORTALTEST1236@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 2	
QEIDMPORTALTEST1237	**Name:** implfirst implllast **Email:** QEIDMPORTALTEST1237@gmail.com **State:** MD	**Account:** Locked **User:** Active	**Group:** FI/Carrier/MAC **Role:** STAR User 10	

Results Per Page First Previous Next Last Showing Page 1 Of 1

6. Help Desk Information

Application Help Desks

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
ASP *(ASP Help Desk)*	844-876-0765	asphelpdesk@dcca.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
CJR *(IBOSC Help Desk)*	844-711-266 *(Option 1)*	CJRSupport@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
CPC (Innovation Center HD) *(Actionet Help Desk)*	N/A	CICDIMServiceDesk@actionet.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

Application *(Help Desk Name)*	Phone	E-mail
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 Help Desk)*	TBD	TBD
FCSO aka The Spot *(FCSO Help Desk)*	855-416-4199	FCSOSpotHelp@FCSO.com
Gentran *(Gentran Support)*	N/A	Gentran-support@cms.hhs.gov
HHVBP *(IBOSC Help Desk)*	844-280-5628	hhvbpquestion@cms.hhs.gov
HIOS *(XOSC)*	855-267-1515	cms_feps@cms.hhs.gov
HPG *(MCARE/ HPG Help Desk)*	866-440-3805	mcare@cms.hhs.gov
IC (Innovation Center) *(Actionet Help Desk)*	N/A	CICDIMServiceDesk@actionet.com
Internet Server *(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	MLMSHelpDesk@cms.hhs.gov
MyCGS *(MyCGS Help Desk)*	866-270-4909	cgs.dme.mac.email.inquiries@cgsadmin.com
Novitas *(Novitas Help Desk)*	877-235-8073	NovitasphereHelp@novitas-solutions.com

Application *(Help Desk Name)*	Phone	E-mail
Open Payments *(Open Payments Help Desk)*	855-326-8366	OpenPayments@cms.hhs.gov
Physicians Value *(PV Help Desk)*	866-288-8912	pvhelpdesk@cms.hhs.gov
PMDA *(PMDA Help Desk)*	443-775-3226	pmda1115_cvp_help@cvpcorp.com
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 *(QualityNet Help Desk)*	866-288-8912	qnet-hd-support-queue@hcqis.org
QMAT *(CEC Help Desk)*	888-734-6433	ESRD-CMMI@cms.hhs.gov
Salesforce *(CMS Salesforce and Force.com)*	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@ffm2.org
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

7. Approver Roles and Functions

Application	Approver Role that can remove role or attribute	Roles that can be removed	Role Attributes that can be removed
COB	COB Approver	COB User	Organization Number
CSR	Authorizer	Approver	Call Center
	Approver	User	Call Center
eRPT	eRPT Authorizer 3	eRPT EPOC	Contract
	eRPT EPOC	eRPT Plan User	
MA/MA-PD/PDP/CC	Authorizer	EPOC	Contract
	EPOC	MA Submitter, MA Representative, PDP Submitter, PDP Representative, MMP User, NET Submitter, NET Representative, MCO POS Edit User, MCO Representative UI Update, Report View, POSFE Contractor	Contract
Novitasphere	Billing Office Approver, Billing Office Approver Back-up, Novitas Solutions Approver, Novitas Solutions Approver Back-up, Provider Office Approver, Provider Office Approver Back-up	Novitasphere End User	Organization
PS&R/STAR	Security Official	End Users, Backup Security Officials	Organization
Quality Domain PV-PQRS	Individual Practitioner	Individual Practitioner Representative	Organization
	Security Official	Group Representative, Web Interface Submitted, PQRS Submitter, PQIP PC Group Representative, PQRS Representative	Organization
	ACO Security Official	Group Representative, Web Interface Submitted, PQRS Submitter, PQIP PC Group Representative, PQRS Representative.	Organization

8. 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
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
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)
GPRO	Group Practice Reporting Option
GUI	Graphical User Interface
HETS	HIPAA Eligibility Transaction System
HPG	HIPAA Eligibility Transaction System (HETS) Provider Graphical User Interface (GUI)
IACS	Individuals Authorized Access to the CMS Computer Services
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

Acronym	Literal Translation
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
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