CENTERS FOR MEDICARE & MEDICAID SERVICES

CMS Enterprise Identity Management (EIDM)

User Guide for Approvers

Working Copy Version 0.2 Release 16 Final

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

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

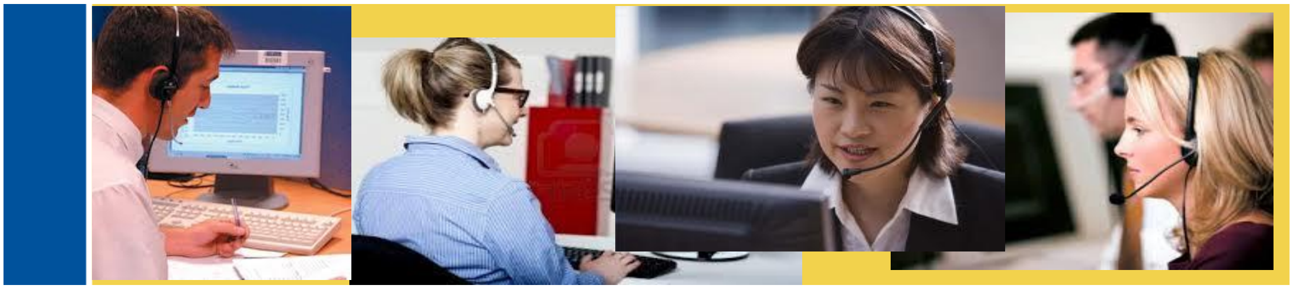
Revision: January 2017

This page is intentionally blank.

Table of Contents

List of Tables

This page is intentionally blank.



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 their 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 User Guide for Approvers"?

The "EIDM User 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

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 by 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

For accessibility options, 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, select **Next**, wait for the program to install, and select **Finish**.

Step 3 Disable your 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.

What You May Need Before Logging In

Prior to requesting access, you should have received instructions from your organization or CMS contact. They 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 one. 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.

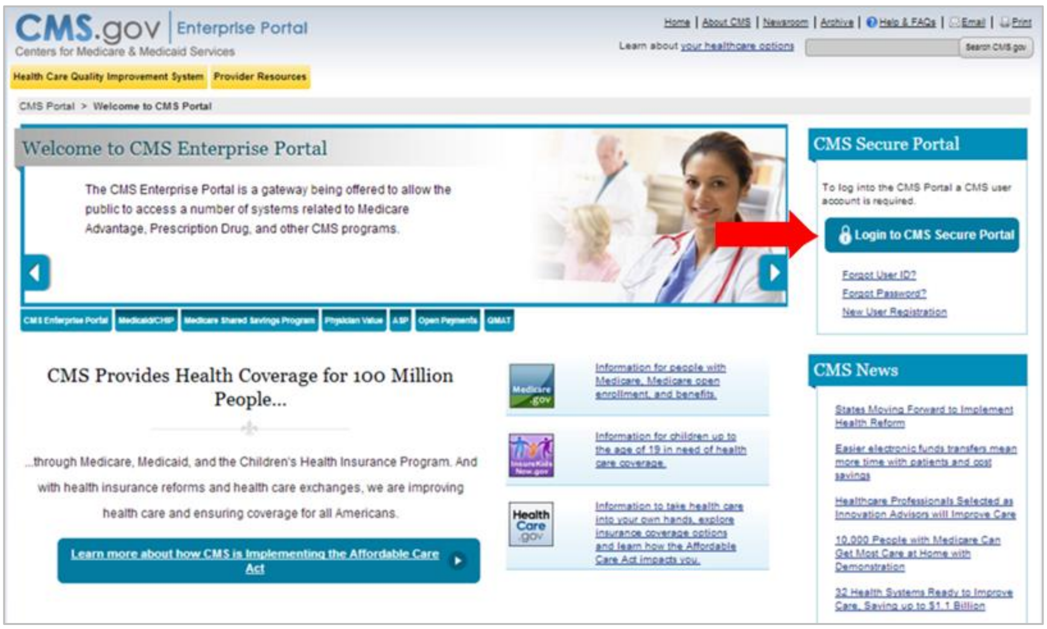
Log into the CMS Enterprise Portal

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

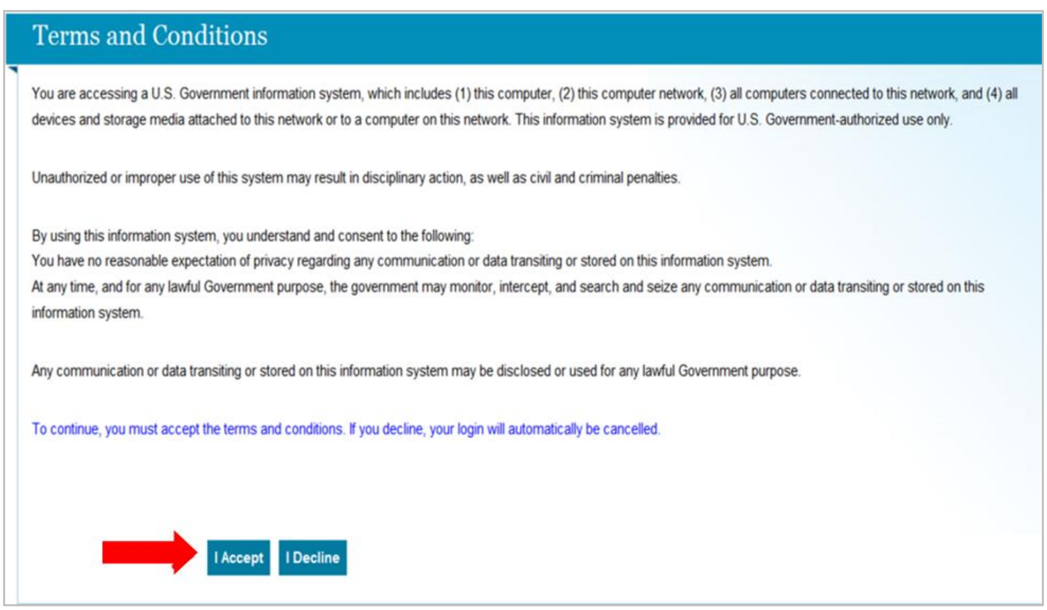
Important Notes

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**.

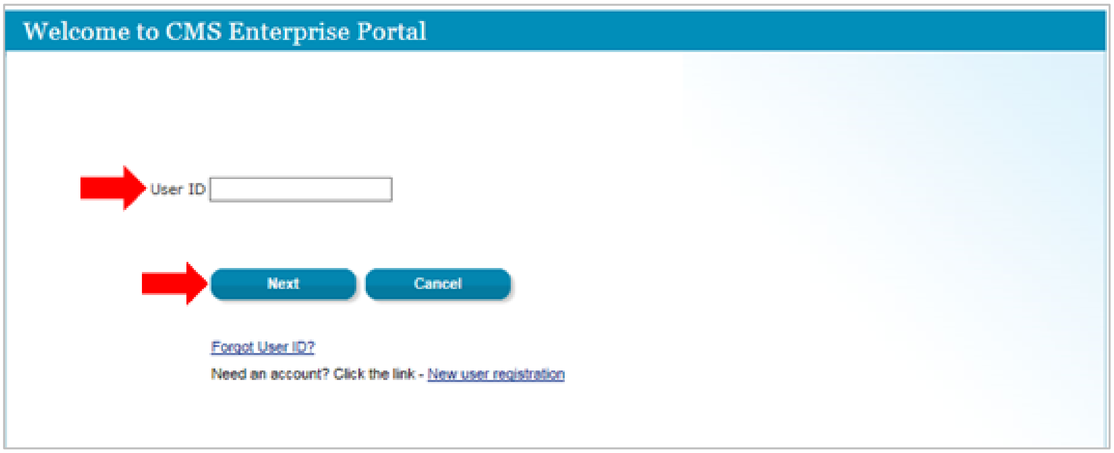


Step 2	Read the “Terms and Conditions” and select **I Accept**.

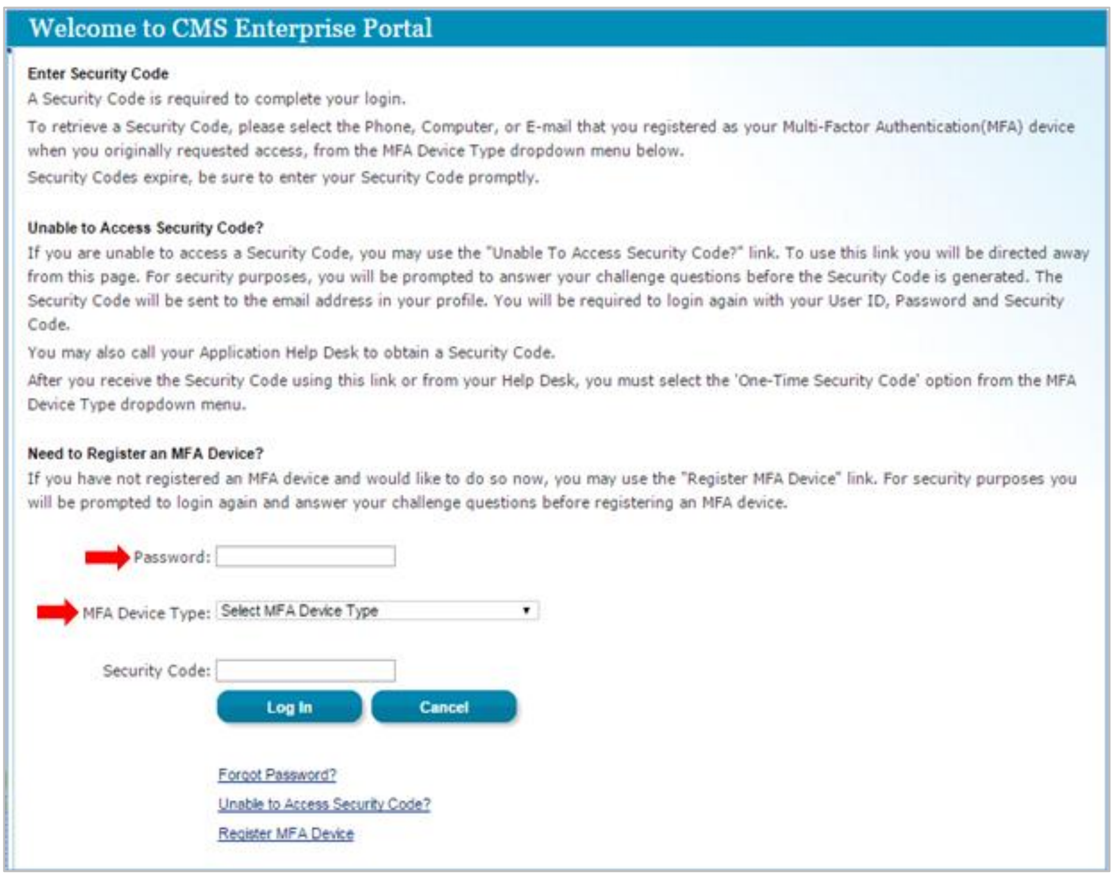


Action

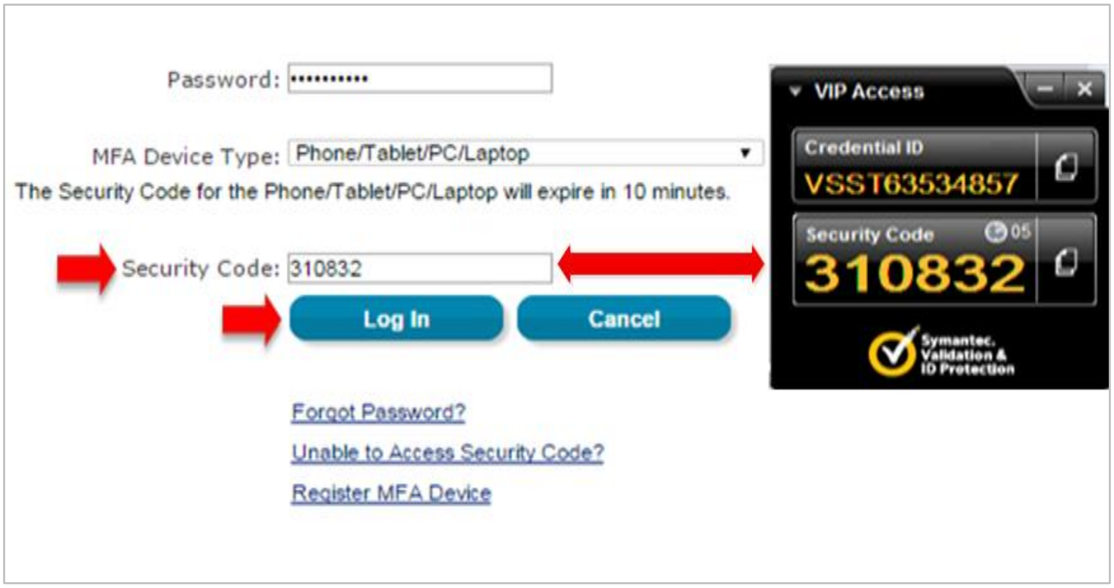
Step 3 Enter your **User ID** and select **Next**.



Step 4 Enter your **Password** and select the **MFA Device Type** for the Multi-Factor Authentication (MFA) device you registered.

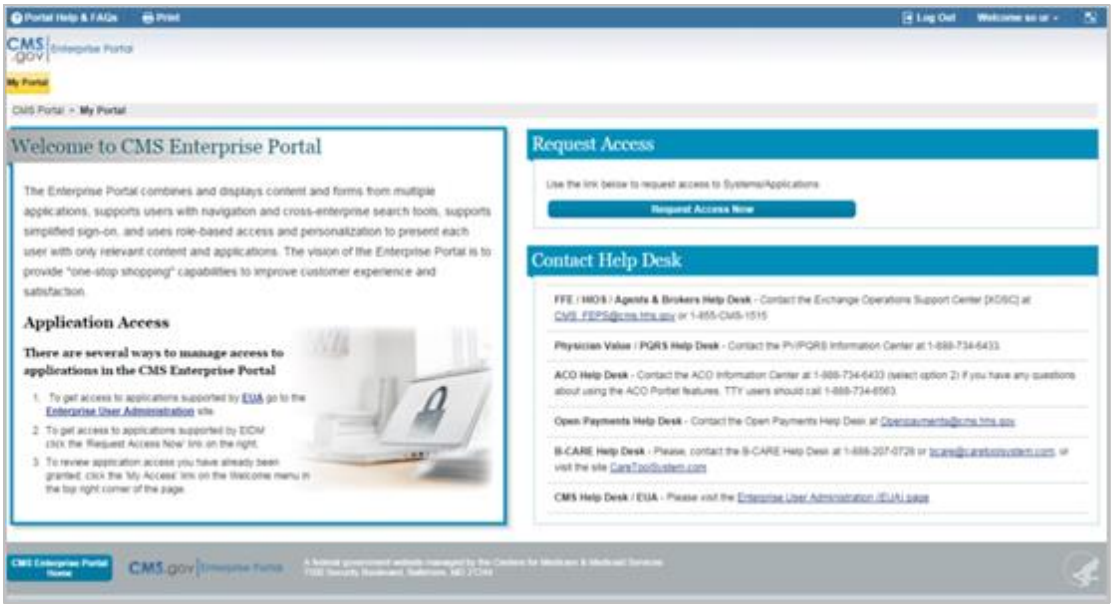


	Action
Step 5	If your **MFA Device Type** is **Phone/Tablet/PC/Laptop**, enter the **Security Code** from your Symantec VIP Access application and select **Log In**. **Note** If you registered a different device, skip to **Step 6**.



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 period, you will need to request a new one.

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



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 checks 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 list to continue. Alternatively, you may **select Request Access Now** to continue.
8. After the **Access Catalog**, **My Access**, and **My Pending Requests** sections display, **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 displays.
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" feature may be used to search for and locate specific pending requests. For example, the "Search" 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 only list pending approvals the approver is authorized to review and approve.
13. **Select** and **view** one or all of the pending requests.
14. After reviewing the information submitted with the request, you can **approve** or **reject** the request. If you approve or reject the request, you must provide a justification for the approval or rejection. Pending requests expire after 60 days unless they are approved or rejected.
15. After a pending request is **approved** or **rejected** by an Approver, an EE-mail notification is sent to the person that submitted the request. The EE-mail includes 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 following applications, **BEGIN HERE**.

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

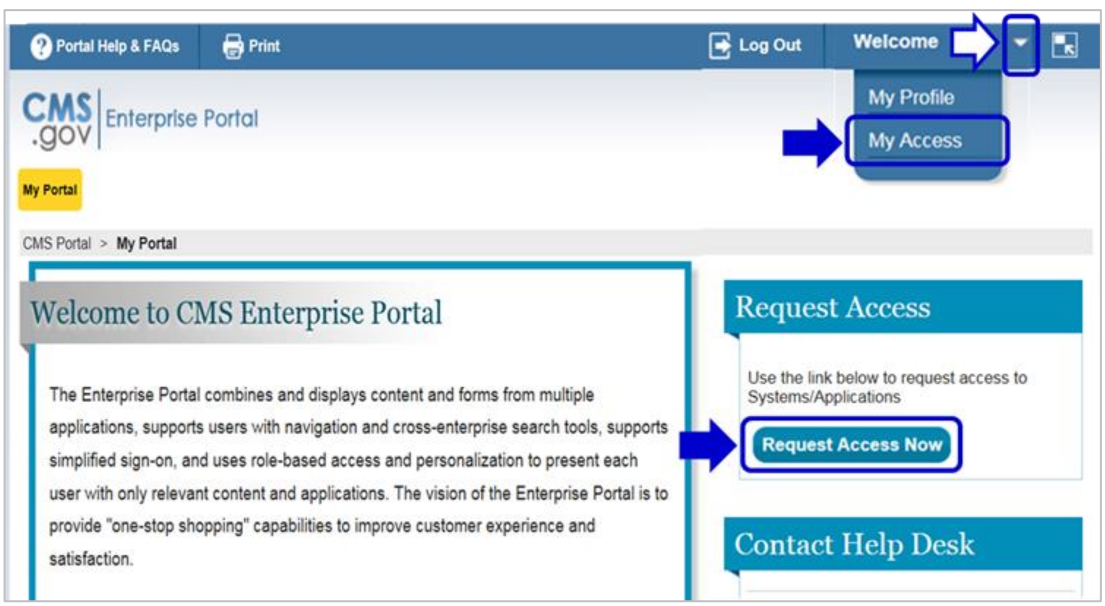
For all other applications, please FOLLOW THESE STEPS.

	Action
Step 1	Log into the CMS Enterprise Portal.

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

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

Note
After logging in, EIDM checks if you are an approver for one or more applications.



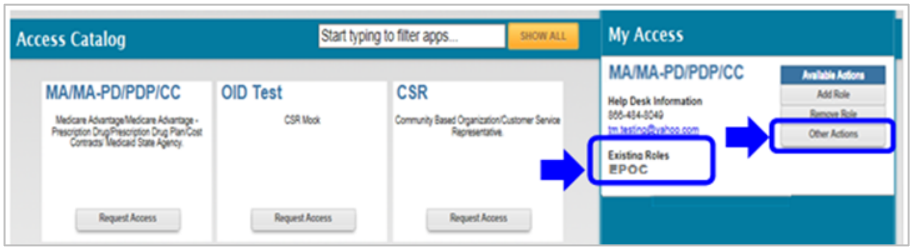
Step	Action

Step 2

The **Access Catalog**, **My Access,** and **My Pending Requests** sections display.

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

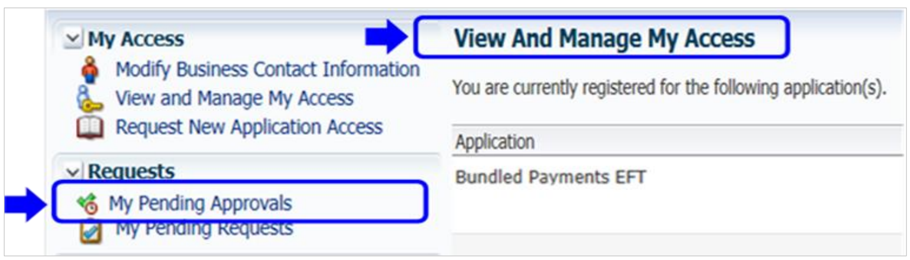
Select **Other Actions** in the **My Access** section to continue. If there are multiple **Other Actions** options displayed, you may select <u>any</u> “Other Actions” option to continue.



Step 3

The **View and Manage My Access** page displays.

Select **My Pending Approvals** to continue.



Step 4

The **Pending Approvals** page displays.

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

The **Pending Approvals** page displays the total number of requests that are pending in your queue.

You may select one or Select All requests that you wish to approve or reject.

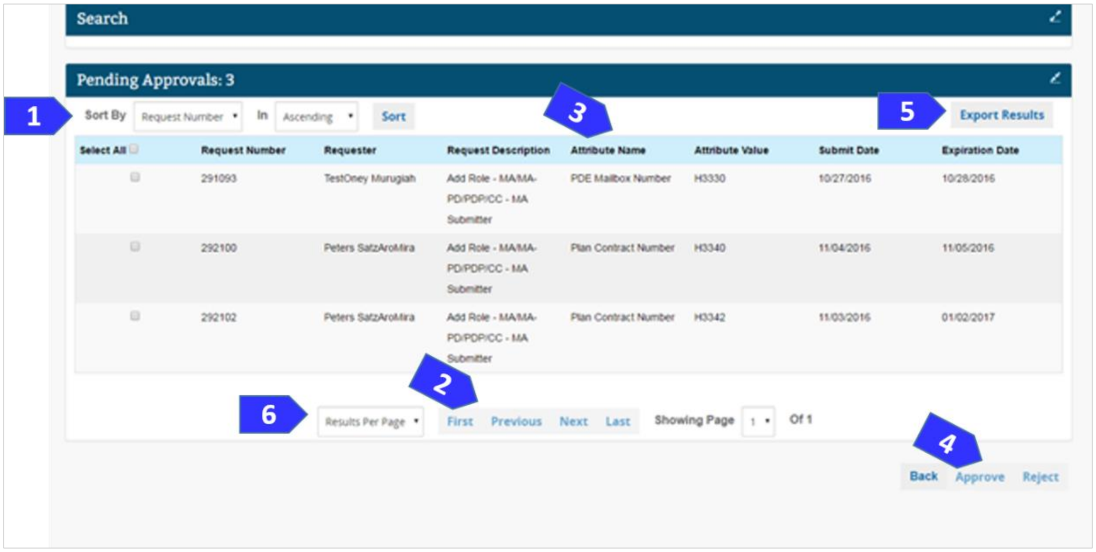
You may also use the **Search** features to narrow your search. Search instructions and tips are provided on the **Pending Approvals** page.

Note (see figure below)

1. By default, the pending requests are sorted in the ascending order for the **Request Number** column. The Approver can sort the pending requests using the **Sort By Dropdown for Requester, Submit Date and Expiration Date** column.
2. The system uses pagination when displaying results. The ability to toggle through pages can be utilized by selecting **First**, **Previous**, **Next**, and **Last**.
3. **Attribute Name** and **Attribute Value** will display the attributes for the roles that require attribute based approval routing.
4. The **Approve/Reject** buttons will be enabled only after one or more request is selected from the checkbox.
5. **Export Results** will print/export all the search results displayed on the **Pending Approvals** page.

Action

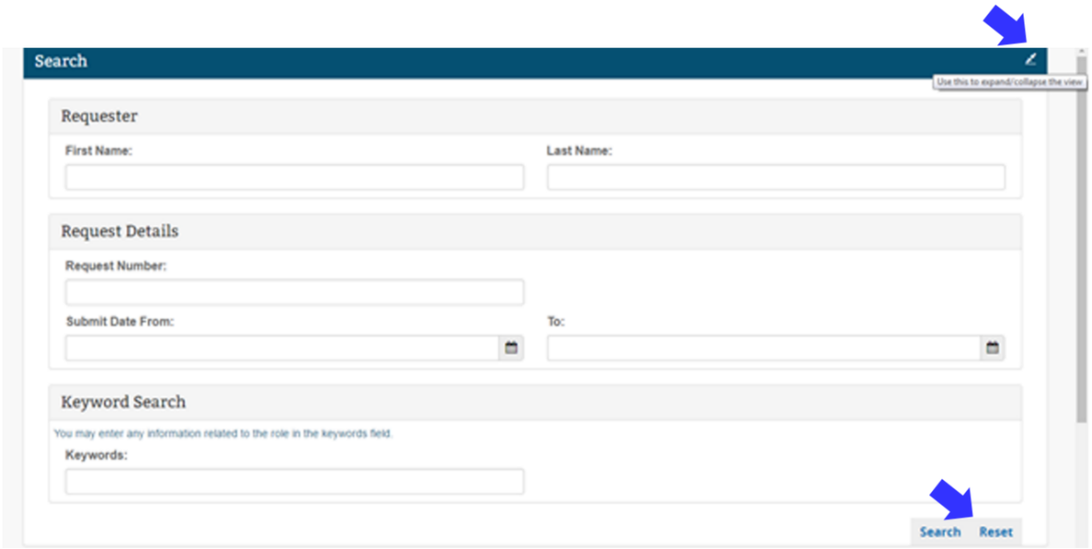
6. Use the "Results Per Page" feature to display up to 20 results per page. By default, it is set to 20.



Select the expandable/collapsible arrow on the rightmost corner to expand the search view.

Entering Search criteria and clicking on the **Search** button will retrieve all the pending requests matching the search criteria.

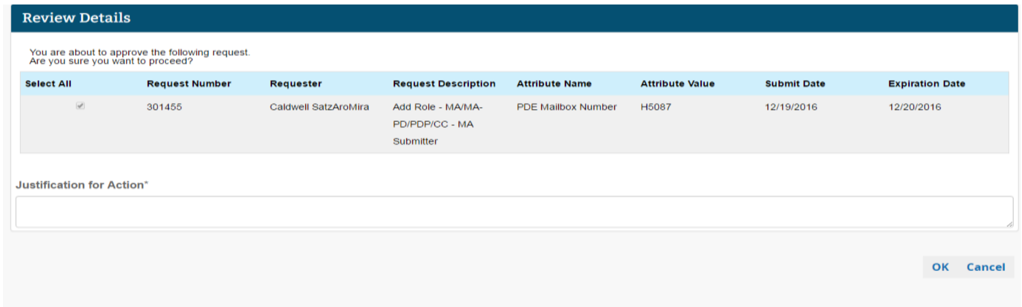
Selecting the **Reset** button will reset the search criteria and the search results.



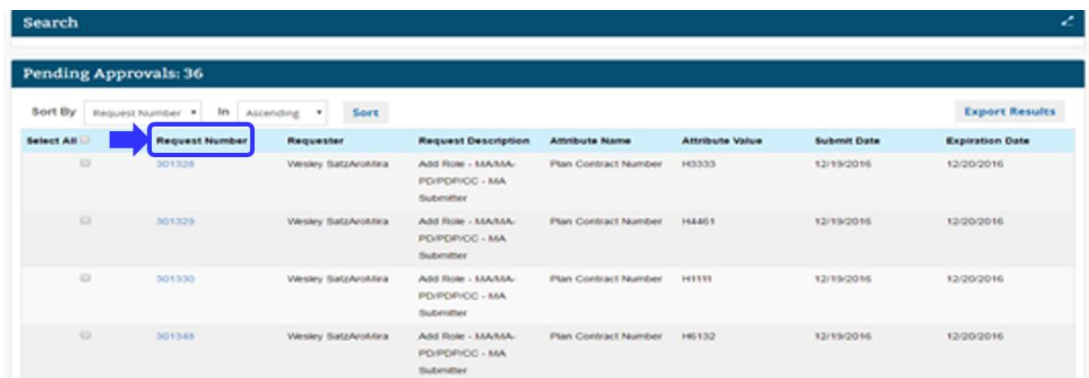
Step 5 After selecting the request and selecting the **Approve or Reject** button, the **Review Details** page will be displayed. This page will be a read-only page. If the request should be *approved*, enter a justification for the approval in the **Justification for Action** box and select **OK** to

Action

approve the request. All information entered into the **Justification for Action** box is 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 **OK** to reject the request. All information entered into the **Justification for Action** box is included in the E-mail sent to the requester.



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



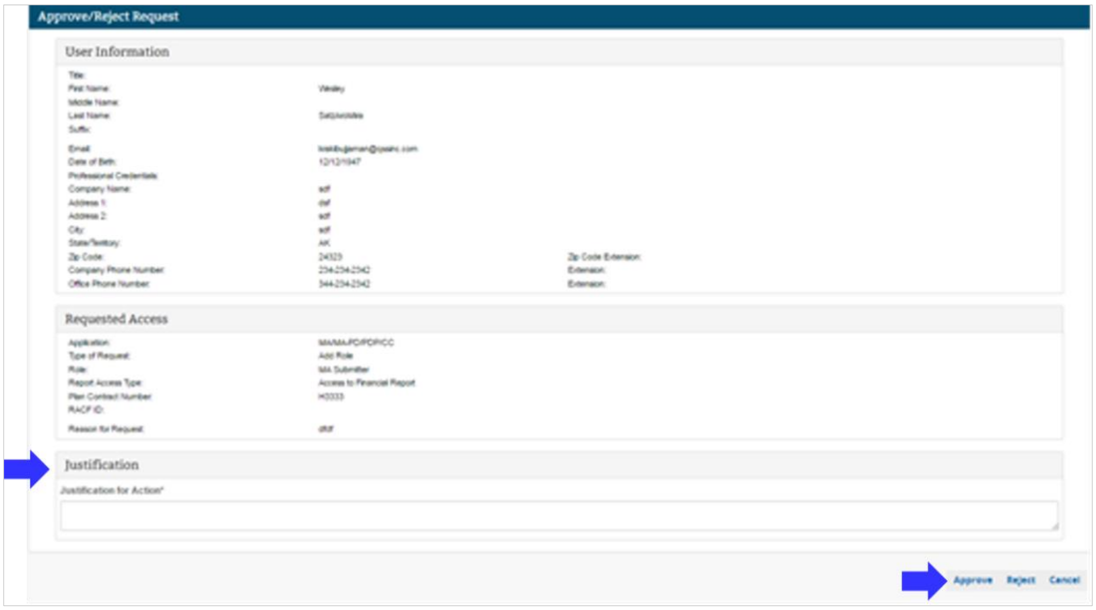
Step 6

Action

The **Approve/Reject Request** page displays.

- 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 is 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 is included in the E-mail sent to the requester.
- If the request should be *cancelled* and no action taken, select **Cancel** to cancel the request and the pending request remains 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 cancellinga request. Any information entered in the **Justification for Action** box is not saved for cancelled requests.

Enter the justification in the **Justification for Action** box and select **Approve**, **Reject**, or **Cancel**.



Step 7 The pending request that you have just approved no longer displays.

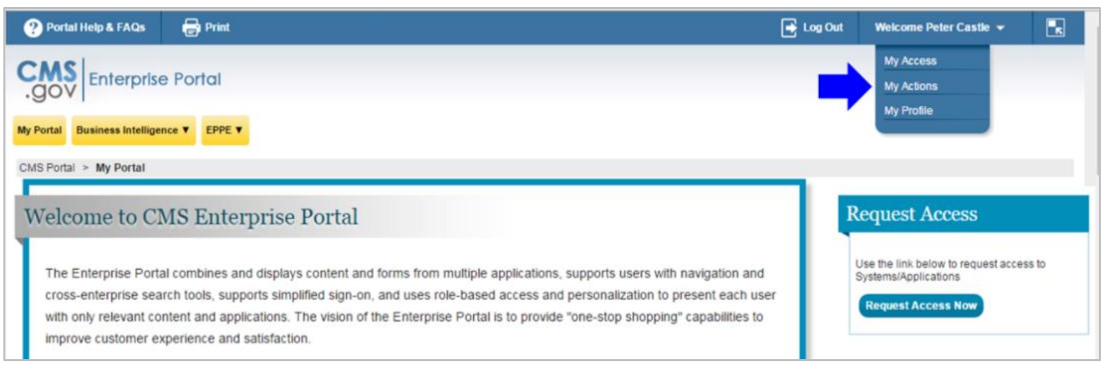
Pending Approvals

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

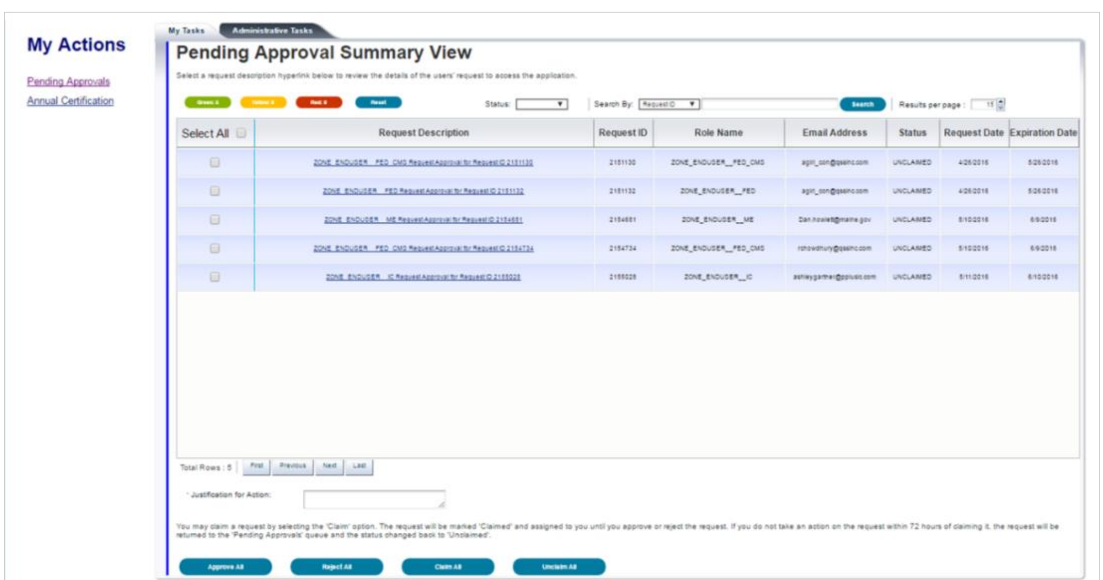
- ASETT
- ASP
- EPPE
- ESD
- IC
- IDHD
- MACPro
- MCU
- MLMS
- Open Payments
- SHIM
- T-MSIS
- zONE

To find, review, approve, reject, or defer a pending request for one of these applications, please FOLLOW THESE STEPS.

	Action
Step 1	Log into the CMS Enterprise Portal. Select the drop-down list located on the top right corner of the home page and select **My Actions**.



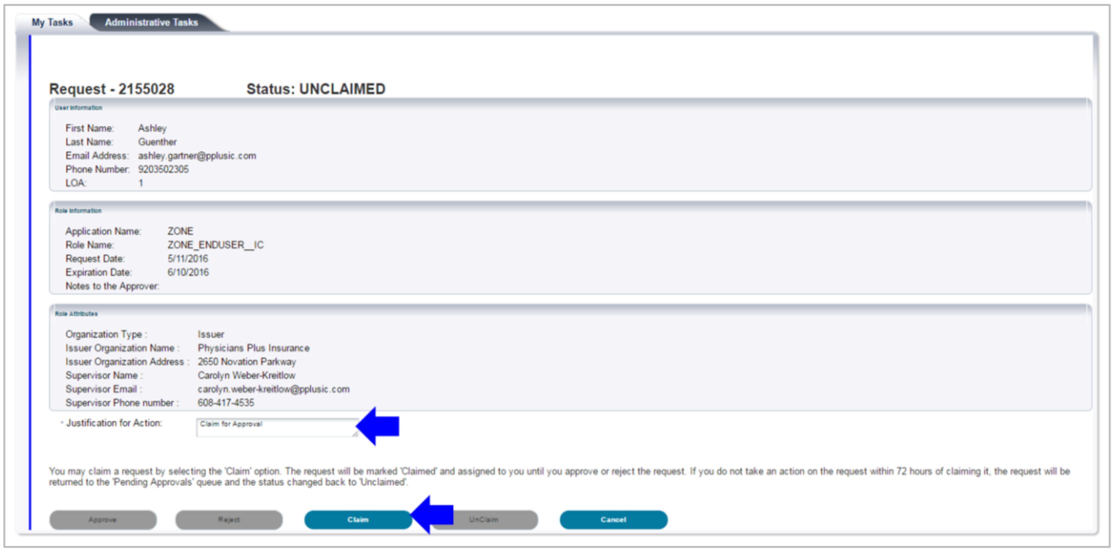
Step 2	The **My Actions** page displays the **Pending Approval Summary View** with the pending approvals queue.



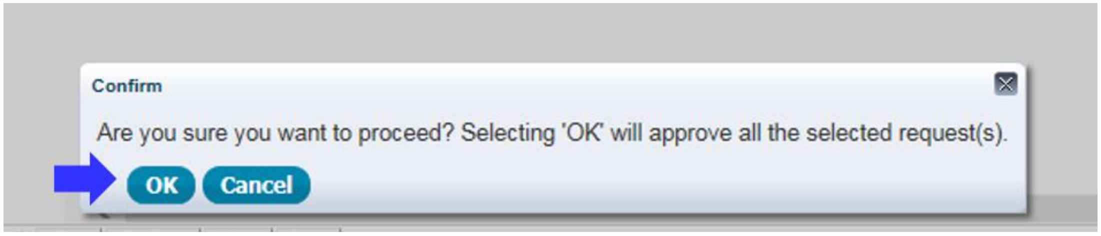
Action

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

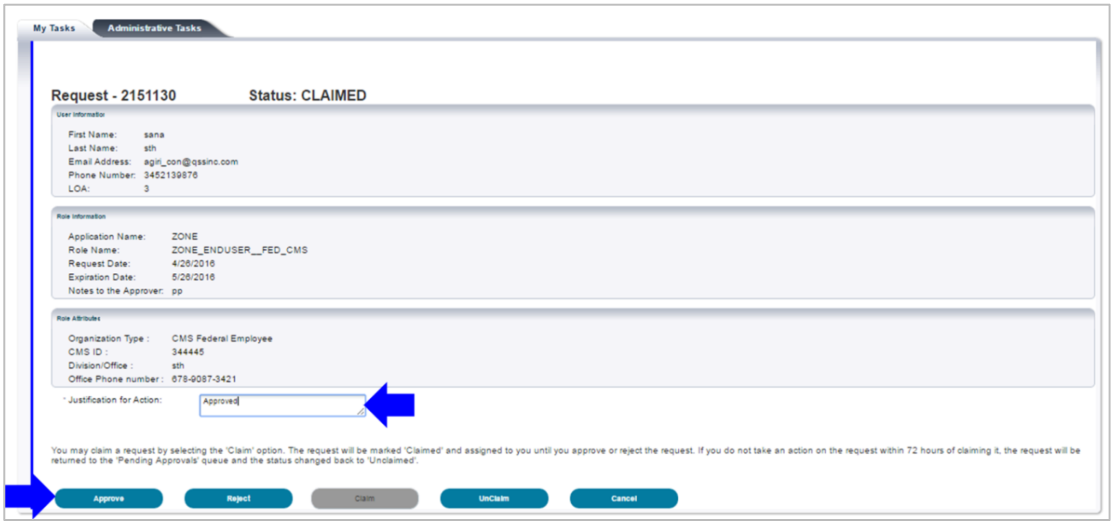
Step 4 In the **Status: UNCLAIMED** window enter a justification for claiming the request in the **Justification for Action** field at the bottom of the page. Select the **Claim** button to continue.



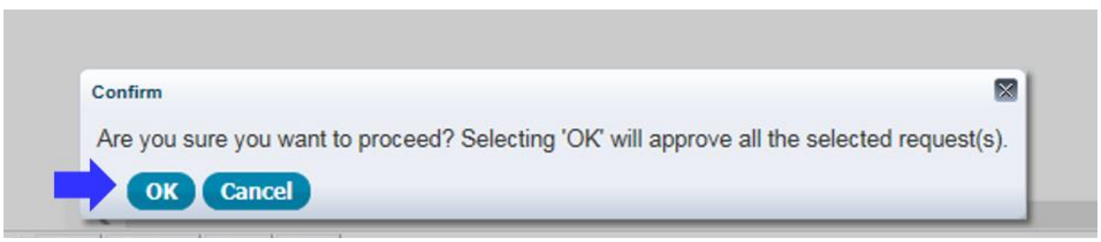
Step 5 Select **OK** to claim the selected request, or **Cancel** to cancel the action, and return to the **Pending Approval Requests Summary** screen.



	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 are removed from the queue.

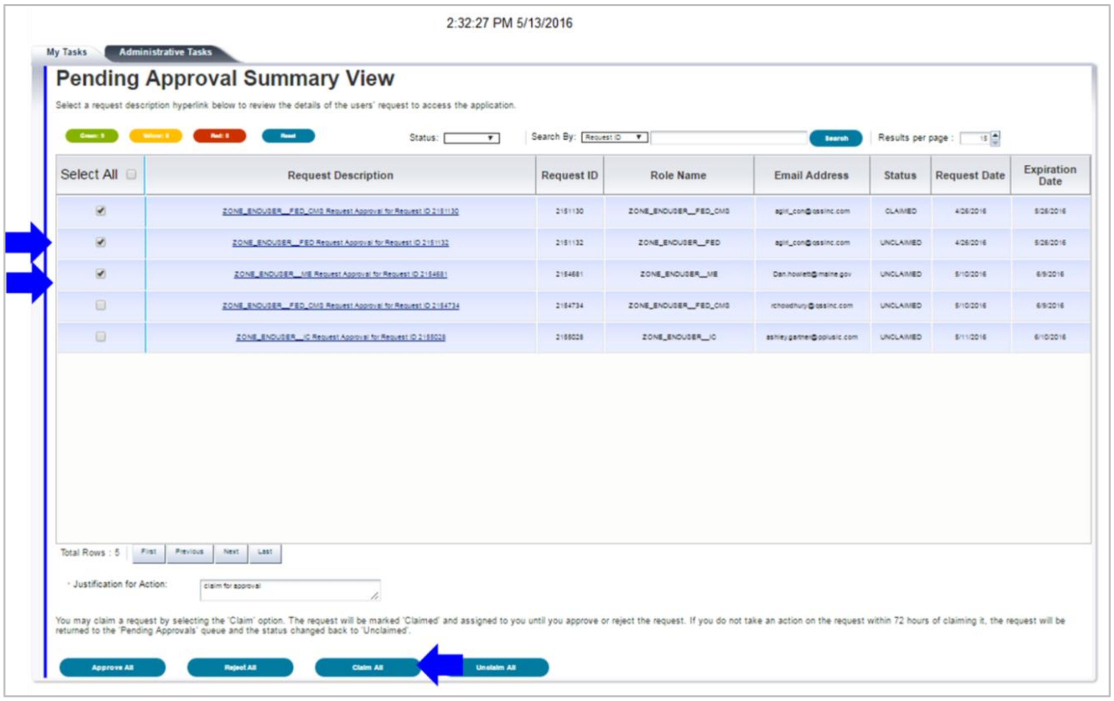
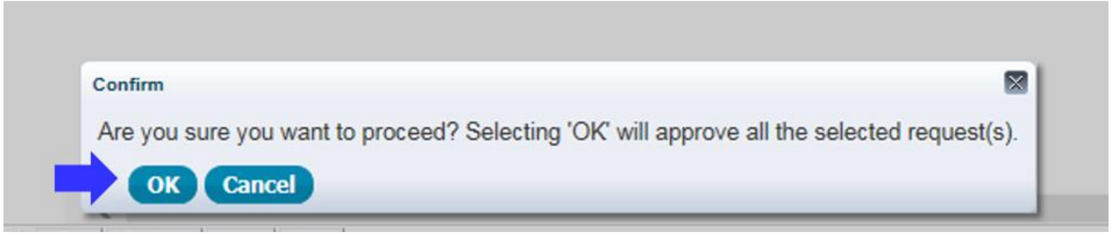
The requestor receives an E-mail with the status of the request. If the request is rejected, the E-mail includes a reason for the rejection.

Mass Approval of Pending Requests

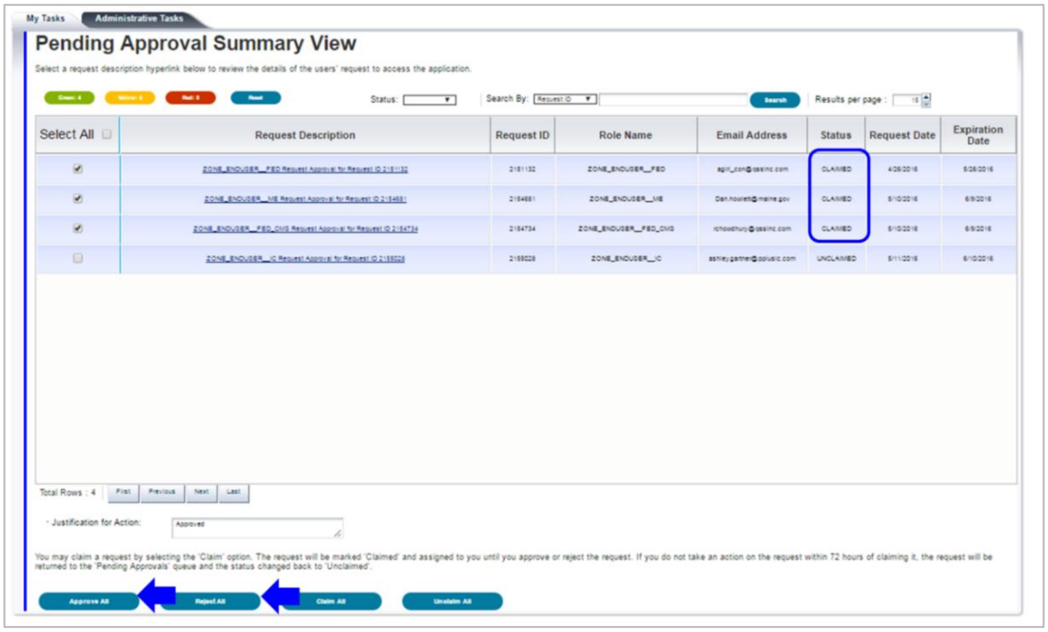
To claim multiple pending requests at once for one of the following applications:

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

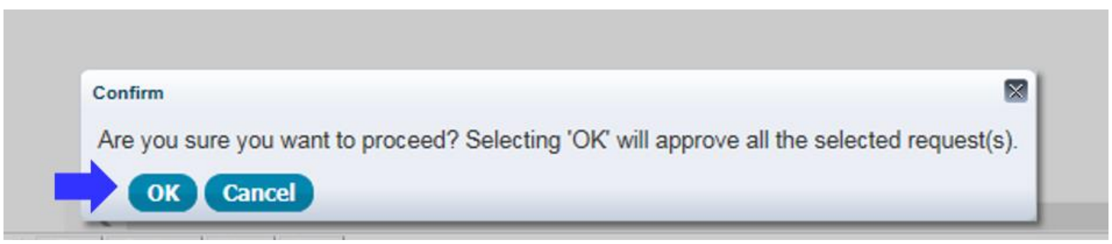
Please FOLLOW THESE STEPS.

	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**.
	
Step 2	Select **OK** to claim all the selected requests and proceed.
	

	Action
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 All** to unclaim the requests.



Step 4	Select **OK** to approve all the selected requests and proceed.

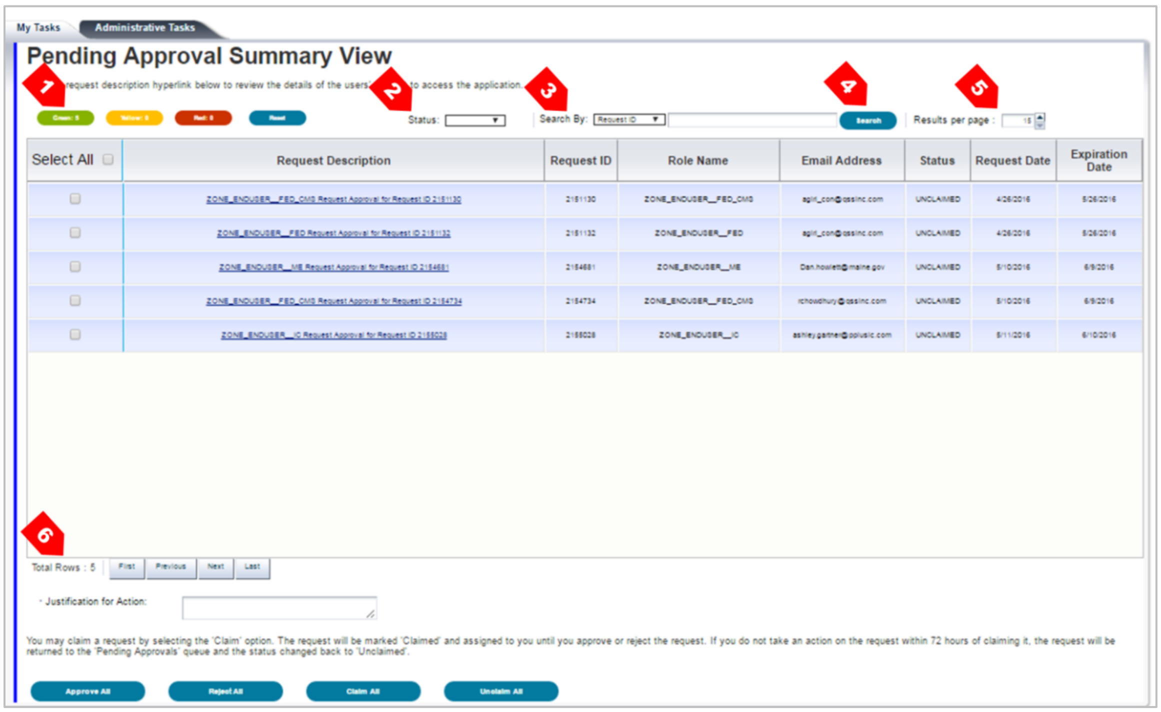


Step	Action
Step 5	A notification displays that the selected role requests are successfully approved.

Features of the Pending Approval Summary Dashboard

The following features of the "Pending Approval Summary Dashboard" display in the image that follows:

1. **Color Status Indicators**:
    a. **Green** – Displays the number of pending requests that expire in 21-30 days
    b. **Yellow** – Displays the number of pending requests that expire within 11-20 days
    c. **Red** – Displays the number of pending requests that expire within 10 days
    d. **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 display
6. **Total Rows**, **First, Previous, Next,** and **Last**: Provide easy navigation through multiple pages



Important Notes
• 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 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.

The CMS Enterprise Portal provides a means to record the Annual Certification actions taken for two types of roles:

1. **Manually Approved Roles**: the original role request requires manual approval by the user with the appropriate authorizing role.
2. **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.

1. 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.
2. 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.

1. 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.
2. 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 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, their users' roles are 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:

1. An Approver for manually approved roles receives an E-mail notifying them that users under their authority are pending Annual Certification. The E-mail provides instructions for completing the certification for users under their authority.
2. The initial E-mail is sent 30 days prior to the certification due date for users requiring manual approval.
3. The system continues to send reminder E-mails to the Approver fifteen (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 EE-mail notification that lists the number of roles pending certification. Follow the instructions in the E-mail to access the **My Users' Certifications** page to certify users' access. The following is a sample E-mail:

Action

From: <donotreply@cms.gov>

Date: Wed, Jul 20, 2016 at 10:15 AM

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 'My Users' Certifications View' tab, select the user for whom you wish to take an action. If you do not find the users in the 'My Users' Certifications 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

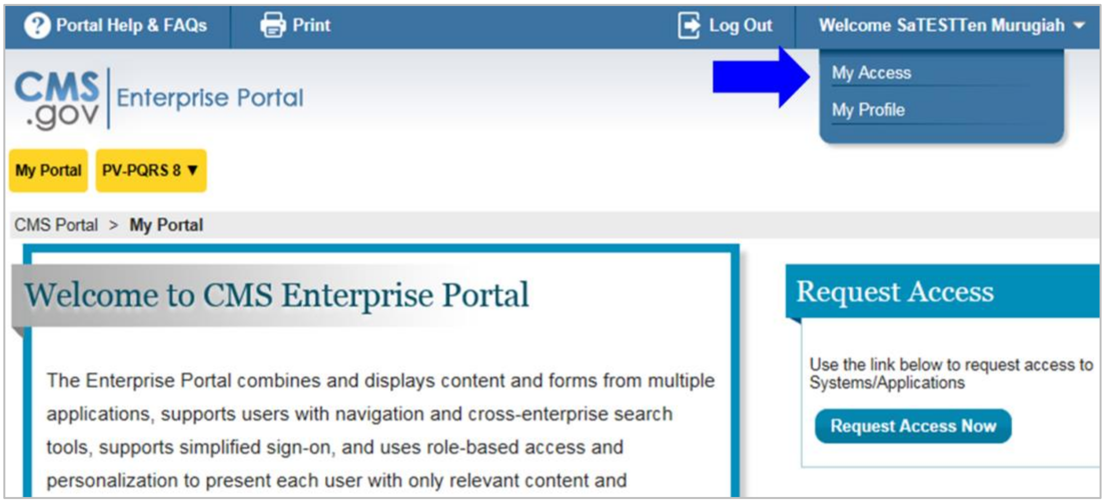
Note

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

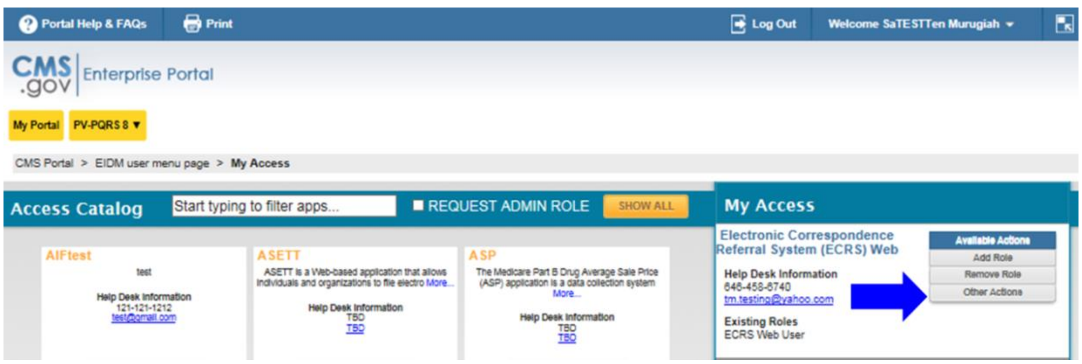
Step 2 Log into the CMS Enterprise Portal.

Select **My Access** in the drop-down list at the top right corner of the Welcome screen.

Action



Step 3 Select **Other Actions** on the **My Access** page.



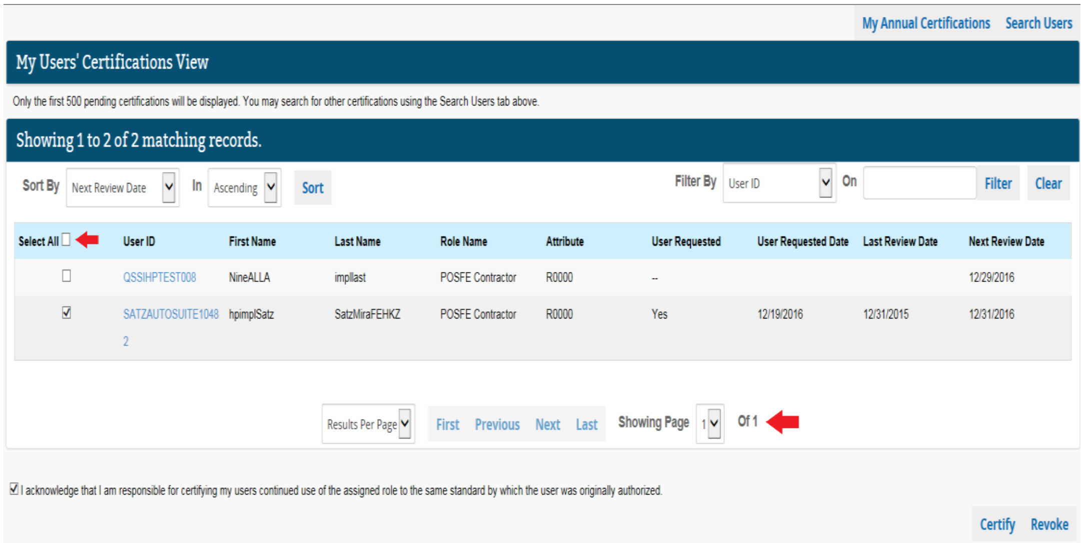
Step 4 The **View and Manage My Access** page displays.

Select the link for **Annual Certification** on the left pane.

	Action
Step 5	The **My Users' Certifications View** page is displayed by default. The approver will have the ability to toggle between the **My Annual Certifications** and **Search Users** tabs.

Select users one by one or in bulk (by checking the **Select All** checkbox) to **Certify** or **Revoke** users' roles.

Only users whose roles are due for certification within the next 30 days are 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.



Notes

- By default, the pending certifications display up to 500 results and are sorted in ascending order by the **Next Review Date** column.
- 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" feature to display up to 100 results per page. By default, it is set to 20.

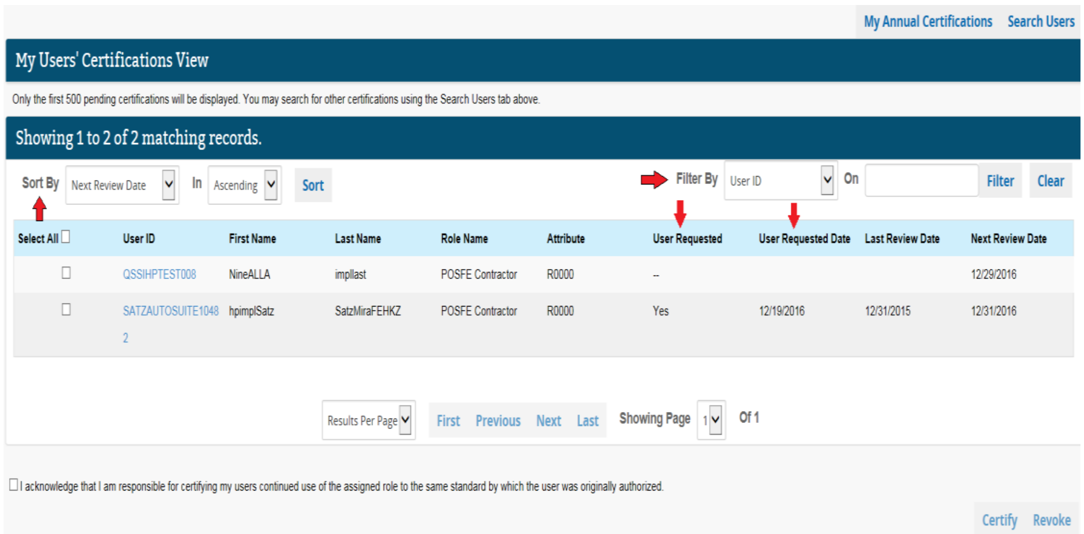
Step 6

The Approver can sort the pending certifications based on the column names using the **Sort By** drop-down in Ascending/Descending order.

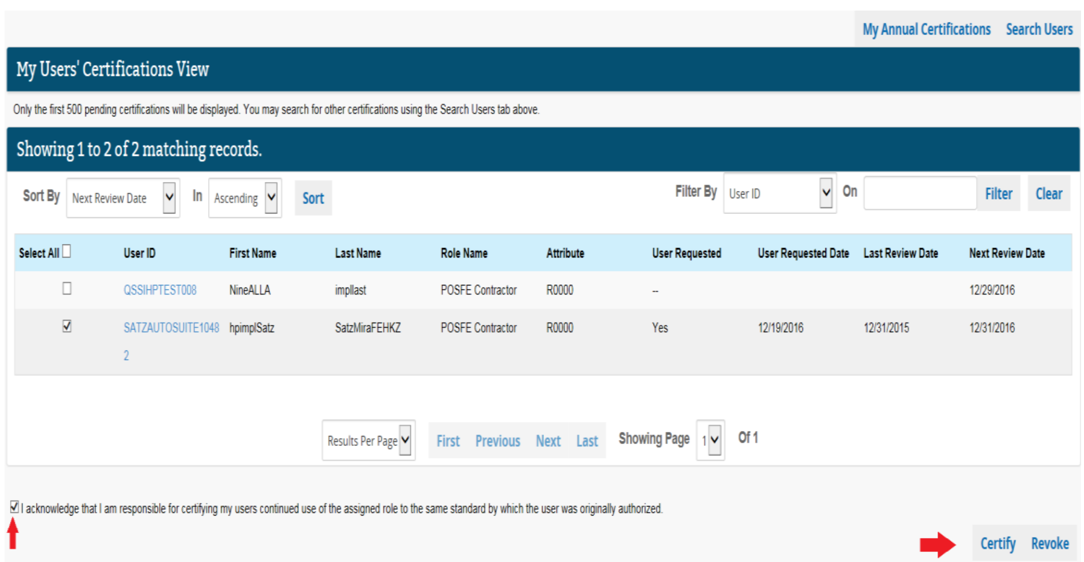
The Approver can filter the pending certifications based on the column names using the **Filter By** drop-down.

The **User Requested** and **User Requested Date** columns will be updated whenever an end user under the approver's authority initiates the annual certification process.

Action



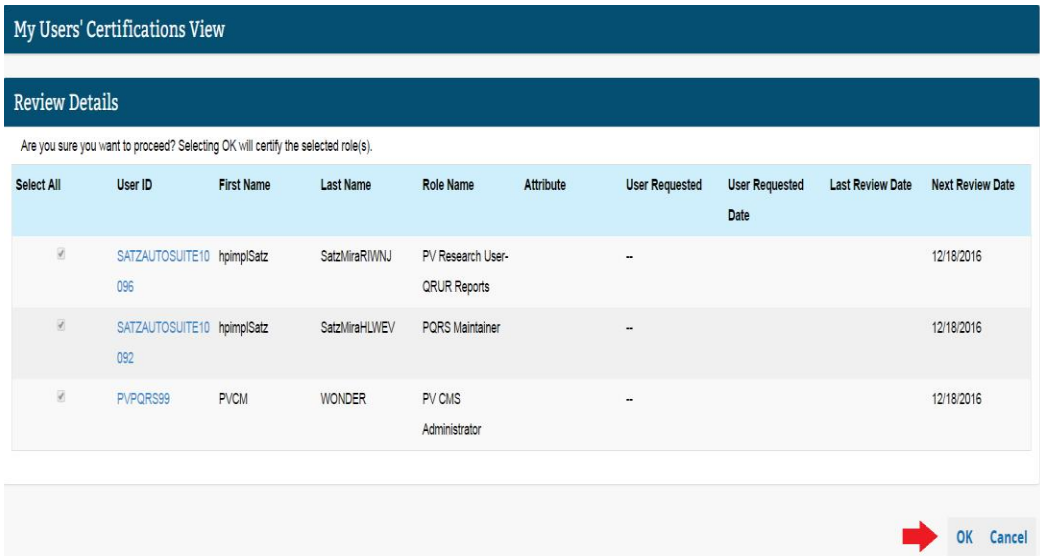
Step 7 Select one or more roles and agree to the acknowledgement statement to certify or revoke the selected user(s). Select **Certify** or **Revoke** to complete the selected user's role certification process.



Notes

- The **Certify** button approves the annual certification of the user's use of a role in an application. An E-mail notification will be sent only to the users who initiated the annual certification process.The **Revoke** button removes the user's role from the application. The user is notified via E-mail when a role is revoked.

	Action
Step 8	A **Review Details** page appears with 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 return to the **My Users' CertificationsView** page.



My Users' Certifications View

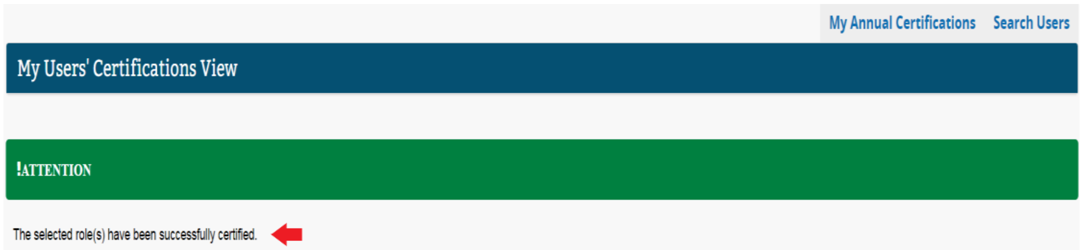
Review Details

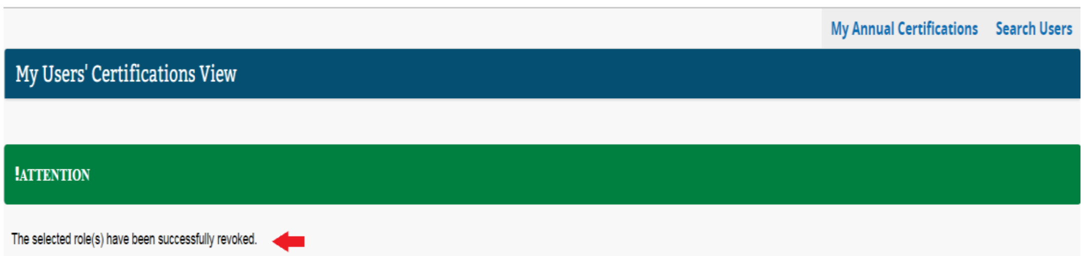
Are you sure you want to proceed? Selecting OK will certify the selected role(s).

Select All	User ID	First Name	Last Name	Role Name	Attribute	User Requested	User Requested Date	Last Review Date	Next Review Date
☑	SATZAUTOSUITE10096	hpimplSatz	SatzMiraRIWNJ	PV Research User-QRUR Reports		--			12/18/2016
☑	SATZAUTOSUITE10092	hpimplSatz	SatzMiraHLWEV	PQRS Maintainer		--			12/18/2016
☑	PVPQRS99	PVCM	WONDER	PV CMS Administrator		--			12/18/2016

OK Cancel

	Action
Step 9	A notification displays in the **My Users’ Certifications View** confirming that the roles have been **Certified** or **Revoked**.





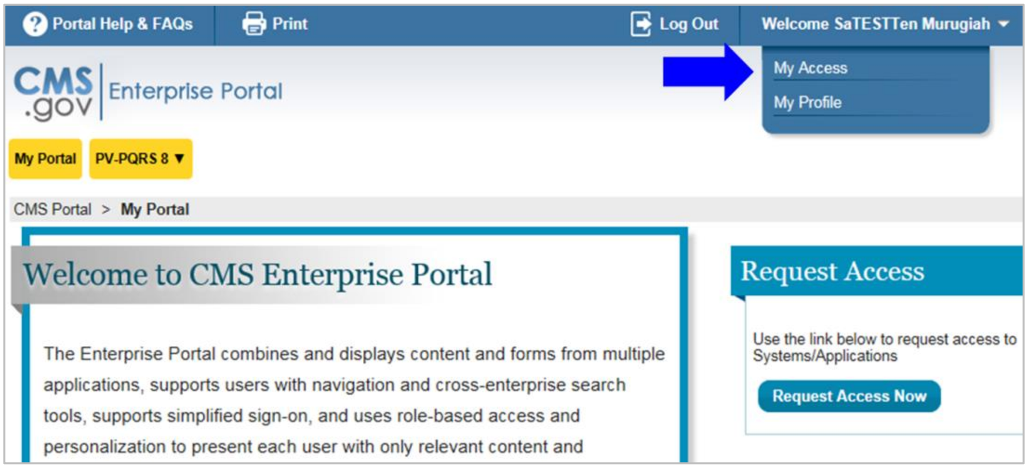
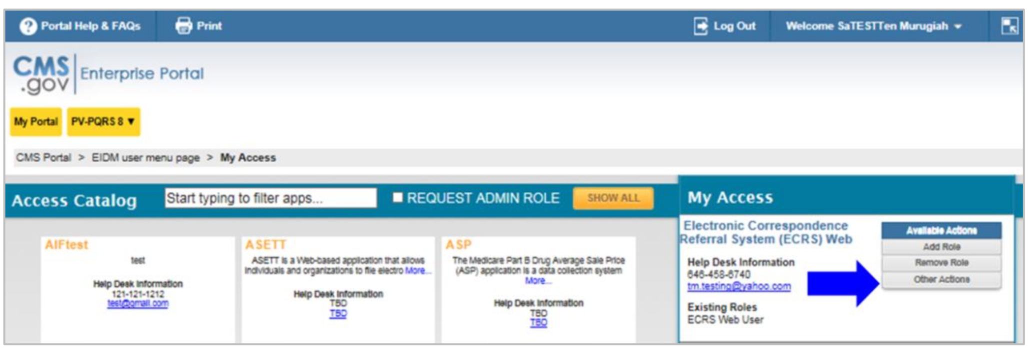
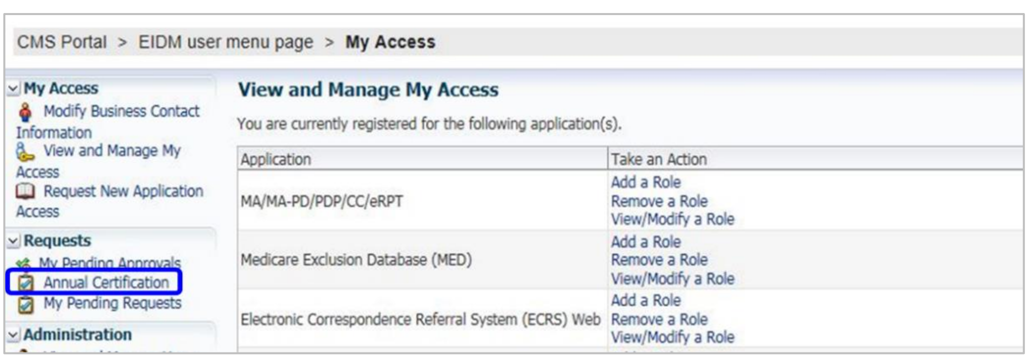
Notes

- The view screen refreshes and the **Next Review Date** is updated for users whose roles were certified.
- The users’ roles that were revoked are no longer included in the pending certifications list.
- Users whose role(s) were removed by the revoke action receive an E-mail with instructions to regain access to the application.
- The E-mail includes Application Help Desk contact information for the application in which the user had the role.

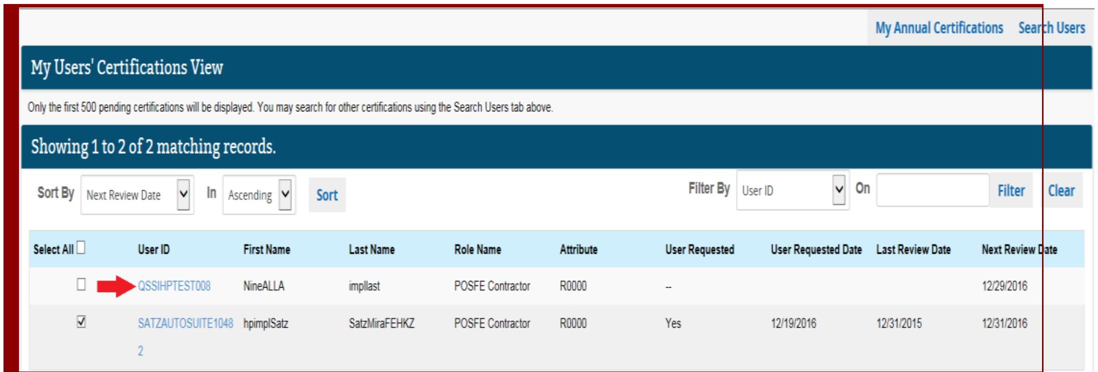
Using the "User Details" Feature

Approvers can view a user's role details and certify or revoke a role for that individual user.

To use the "User Details" feature, FOLLOW THESE STEPS:

	Action
Step 1	Log into the CMS Enterprise Portal. Select **My Access** in the drop-down list at the top right corner of the Welcome screen. 
Step 2	The **My Access** page displays. Select **Other Actions**. 
Step 3	The **View and Manage My Access** page displays. Select the link for **Annual Certification** on the left pane. 

	Action
Step 4	The **My Users' Certifications View** page displays. Select a user by selecting their **User ID**.

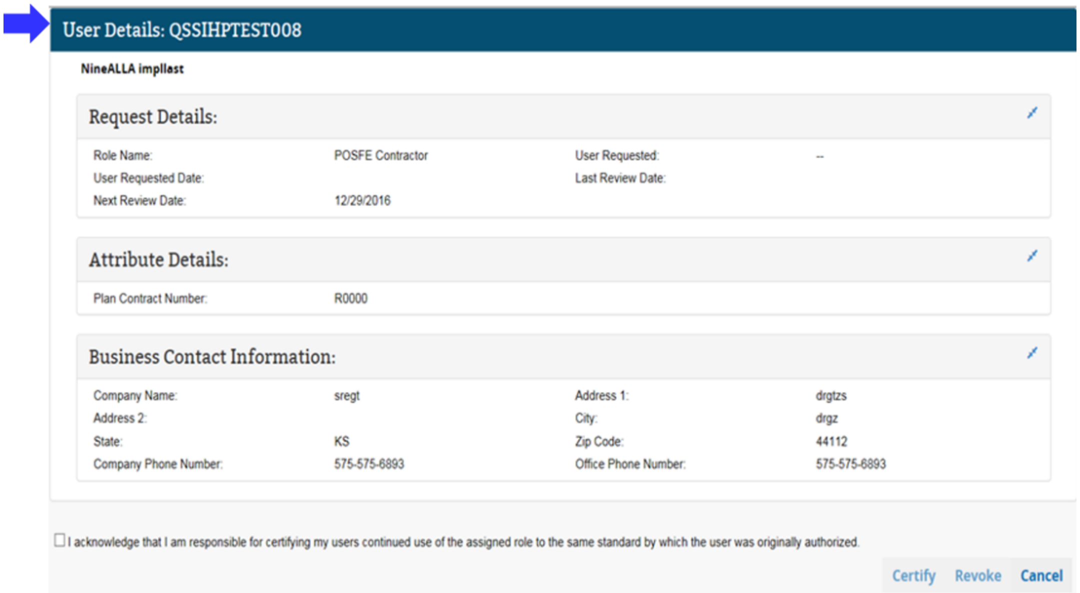


Notes

- Only users whose roles are due for certification within the next 30 days are 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 default, the pending certifications display up to 500 results and are sorted in ascending order by the **Next Review Date** column.
- The Approver can sort the pending certifications based on the column names using the **Sort By** drop-down in Ascending/Descending order.
- The Approver can filter the pending certifications based on the column names using the **Filter By** drop-down.
- 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" feature to display up to 100 results per page. By default, it is set to 20.

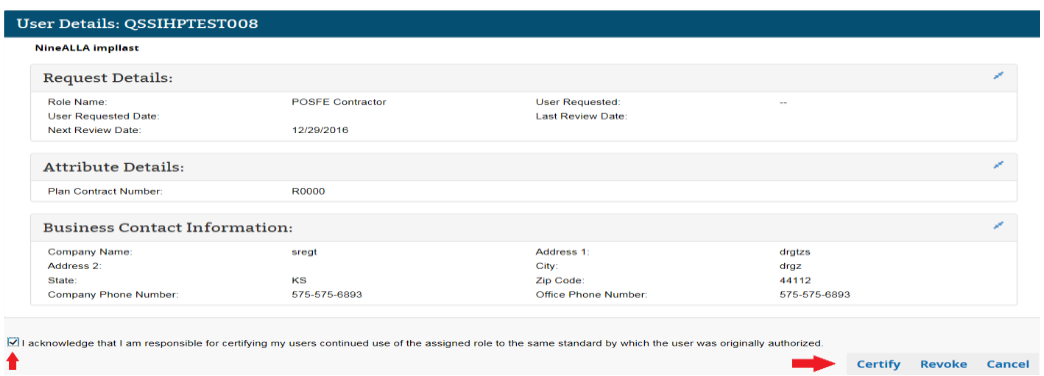
Step 5	The **User Details** page displays.

Action



Step 6

Agree to the acknowledgement statement to Certify or Revoke the user. Select **Certify** or **Revoke** to complete the pending user's role certification.



Notes

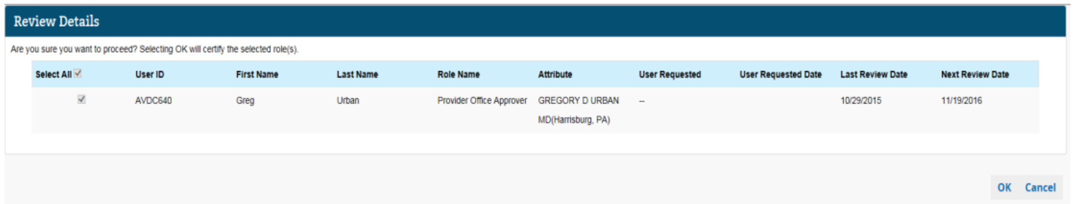
- **Certify** approves the Annual Certification of the user's role in an application.
- The end users who have initiated the Annual Certification process will be notified via E-mail when the role is approved.
- **Revoke** removes the user's role from the application. The user is notified via E-mail when a role is revoked.

Step 7

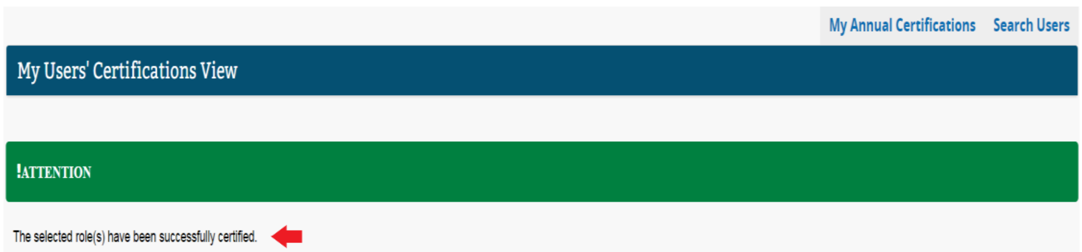
A **Review Details** page displays for you to confirm that you want to certify or revoke the role.

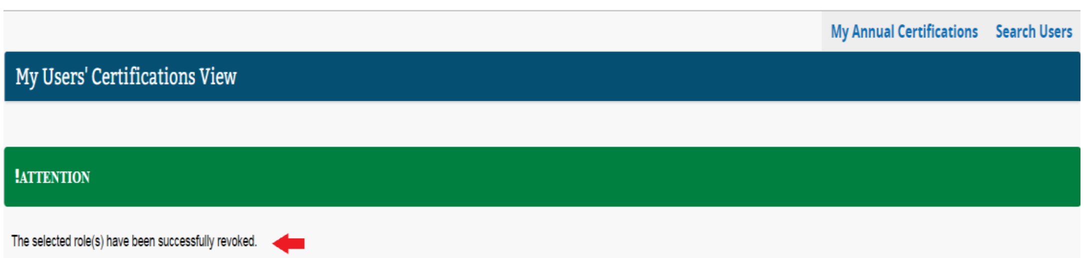
Confirm the action by selecting the **OK** button. Select the **Cancel** button to cancel the action and to return to the **User Details** page.

Action



Step 8 A notification displays in the **My Users' Certifications View** confirming that the roles have been **Certified** or **Revoked**.



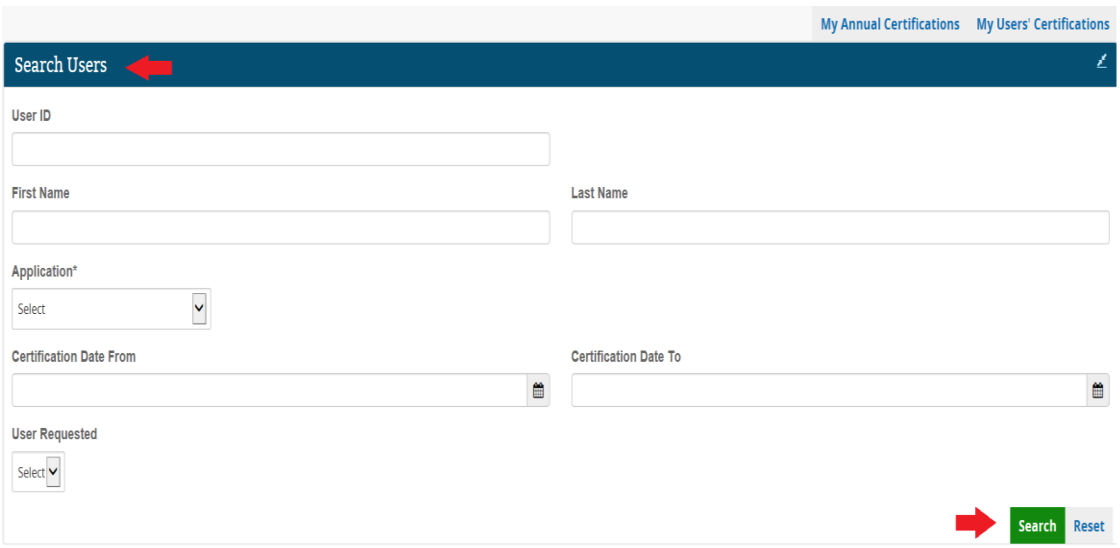


Using the "Search Users" Feature

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 populates 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.



Note

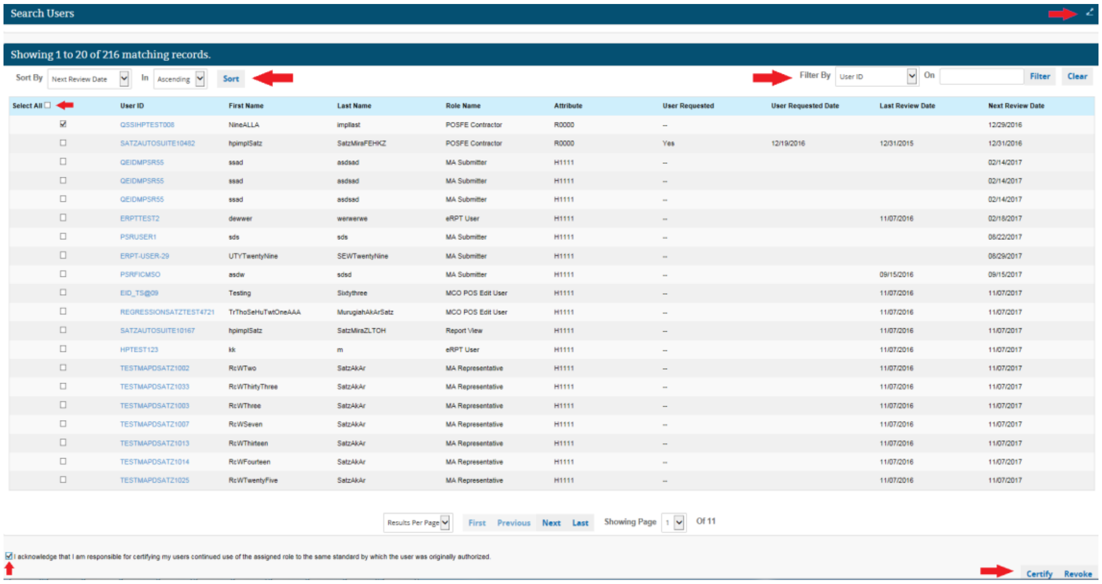
The following characters are not allowed in any of the search fields: Asterisk (*), Percentage (%), Double quotation mark ("), Ampersand (&), Cap (^), Less-than sign (<), and Greater-than sign (>).

- **User ID, First Name, and Last Name**: Enter a minimum of two (2) characters in the search field.
- **Application**: If you are an approver for only one application, the application name is pre-selected by default and is 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 applications that are under your approval authority. If you are an approver for only one role in the application, the role is pre-selected by default and is grayed out.
- **Certification Date From and To:** Enter a date in mm/dd/yyyy format, or select a date to search pending certifications. The From date cannot be past 365 days from the current date.

Action
• **User Requested:** Select from the drop-down list options of 'Yes' and '—'. • **User Requested Date From and To:** This field is displayed whenever a user selects 'Yes' on the **User Requested** field. Enter a date in mm/dd/yyyy format, or select a date to search the user requested date. The From date cannot be past 365 days from the current date.

Step 2	Action

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.



Notes

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 500 results are populated. All pending certifications that are due up to the next 365 days can be viewed.

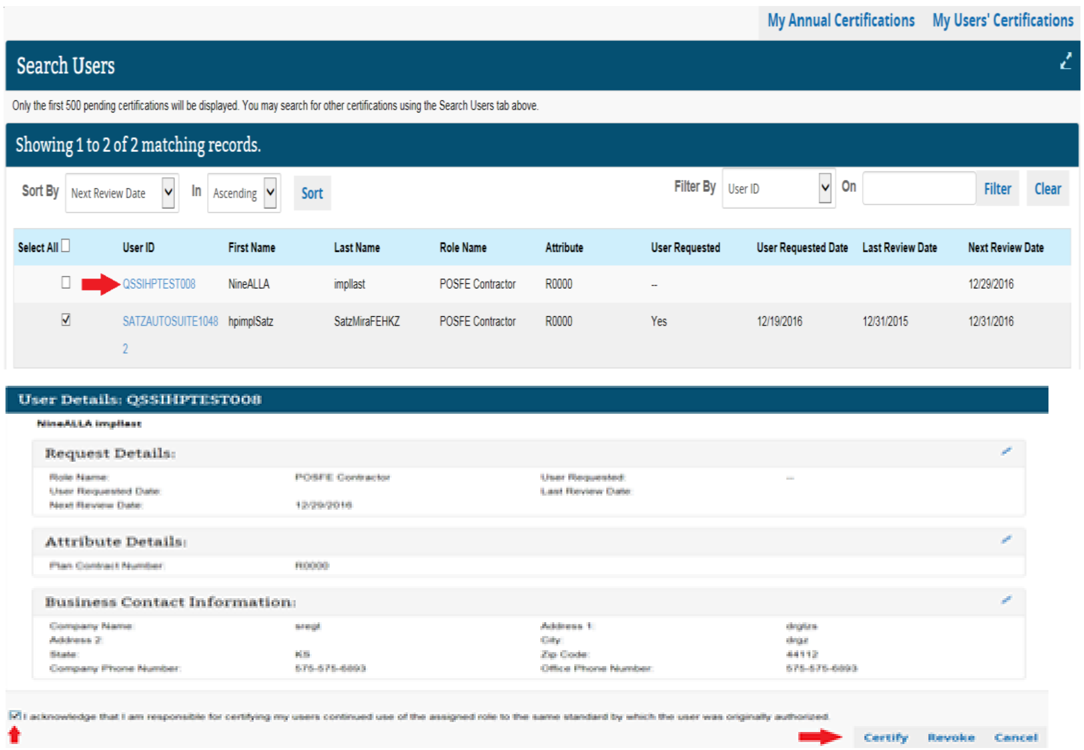
The system uses pagination when displaying results. The ability to toggle through pages can be utilized by selecting **First**, **Previous**, **Next**, and **Last**.

Use the "Results Per Page" feature to display up to 100 results per page. By default, it is set to 20.

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
- **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.
- **User Requested**: This field is updated when an end user submits a request to initiate the Annual Certification process.
- **User Requested Date**: The date an end user submits a request to initiate the Annual Certification process.
- **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

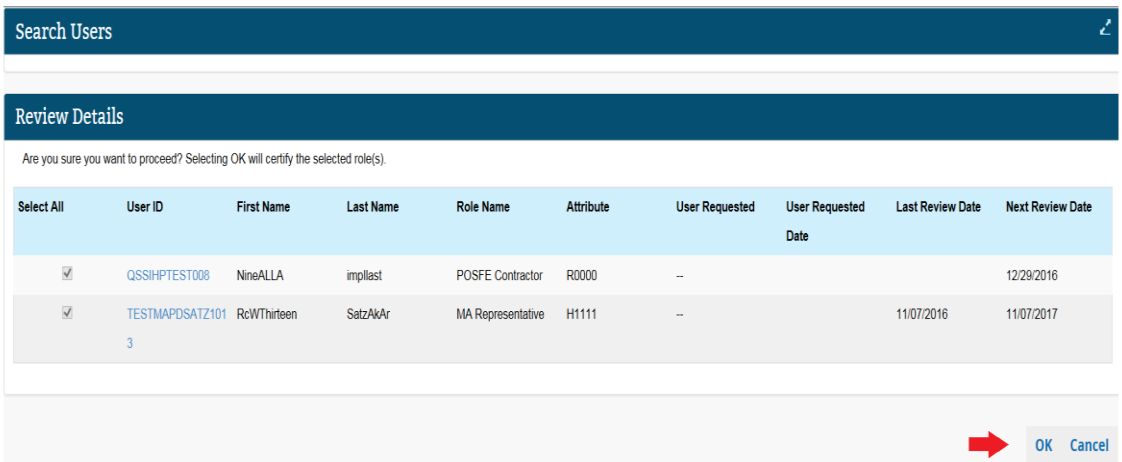
	Action
	maintained in a trusted resource that requires trusted resource validation. It displays only when the trusted resource validation fails.
Step 3	Select the User ID hyperlink to view the **User Details** page. Agree to the acknowledgement statement to Certify or Revoke the selected user(s). Select Certify or Revoke to complete the pending user's role certification.



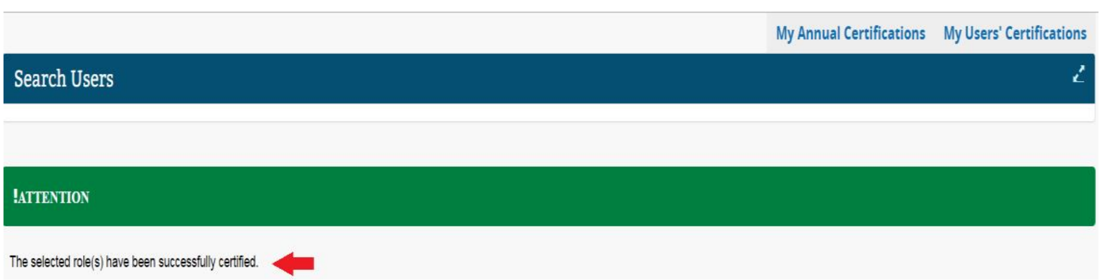
Notes

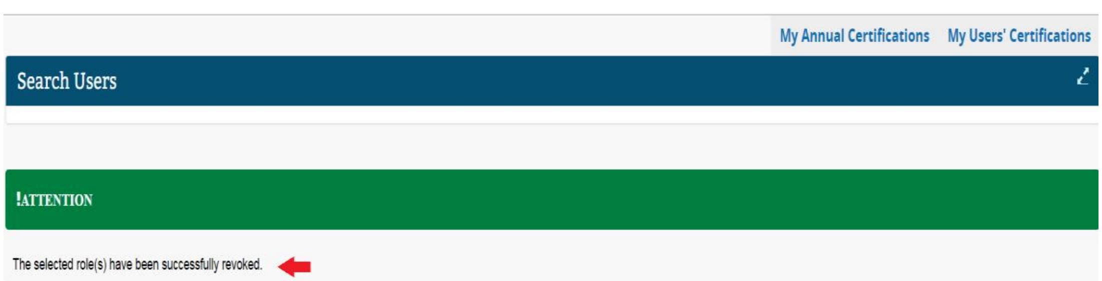
- The **Certify** button approves the Annual Certification of the user's use of a role in an application.
- The **Revoke** button removes the user's role from the application. The user is notified via E-mail when a role is revoked.

	Action
Step 4	A **Review Details** page 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 be certified or revoked. Confirm the action by selecting the **OK** button. Select the **Cancel** button to cancel the action and return to the **Search Users View** page.



Step 5	After certifying or revoking the roles, a notification displays in the **Search Users View** confirming that the roles have been **Certified** or **Revoked**.





Action

Notes

- The user receives an E-mail when either the Approver revokes the role access or when the Approver does not take action 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 E-mail.

The following is a sample E-mail:

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 the 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 receives an E-mail notification.

Some examples include:

- Users Failed Validation Check – Approver E-mail Notification
- Users' Roles Removed – Approver E-mail Notification
- Users' Roles Removed – User E-mail Notification

Users Failed Validation Check – Approver E-mail Notification

Approvers who are responsible for users with validated roles receives the initial E-mail 90 days prior to the Annual Certification due date. This E-mail includes the users and roles that failed the validation check.

Reminder E-mails 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. The following is a sample E-mail:

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.

Important Notes

- If the user's account failed the validation check by the certification due date, their role is removed and the user is notified by E-mail.
- If the user's account passed the validation check, then the role passed Annual Certification until the next certification due date. No E-mails 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 E-mail Notification

Approvers who are responsible for users who have validated role(s) receive an E-mail informing them of their users' role removal, when a validated role fails Annual Certification due to failing the validation check. The following is a sample E-mail:

> **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.

Important Note
Instructions for regaining access to the application are provided in the E-mail.

Users' Roles Removed – User E-mail Notification

Users with validated roles who failed Annual Certification receive an E-mail notifying the user of their role being removed. The following is a sample E-mail:

> **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.

Important Note
Instructions for regaining access to the application are provided in the E-mail.

Account Review

In order to prevent the unnecessary accumulation of unused user accounts, CMS periodically checks whether the user accounts are still needed and are actively being used. If any account has a role associated to it, it is considered active and is not subject to account review. User accounts that do not have any roles associated to it may be removed based on the inactivity period described below.

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 is 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 of the following statements are true:
  - The User's account does not have a role in any application.
  - The 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 following table:

EIDM Checks Performed		Result	Next Steps/Action Taken
1.	Does the account have a role?	Yes	Account review passes. No further action is taken.
		No	Proceed to next step.
2.	Has the account been inactive for less than 180 days?	Yes	Account review passes. No further action is taken.
		No	Proceed to next step.
3.	Has the account been inactive for 180 days or more but less than 360 days?	Yes	Account review fails. User is notified by E-mail.
		No	Proceed to next step.
4.	Has the account been inactive for 360 days or more?	Yes	Account review fails. Account is deleted. User is notified by E-mail and may re-register in EIDM.

Table 1: Account Review Checks

Account Fails Review at 180 Days

In the event an account fails review at 180 days, the account is locked and an E-mail is sent to the user. The following is a sample E-mail:

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.

Important Note

Locked users can unlock using the self-service function by answering the challenge questions that they set up 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 is deleted and an E-mail is sent to the user. The following is a sample E-mail:

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.

Important Note

The E-mail includes instructions to regain access to the CMS Enterprise Portal by registering for a new user account.

5. User Management

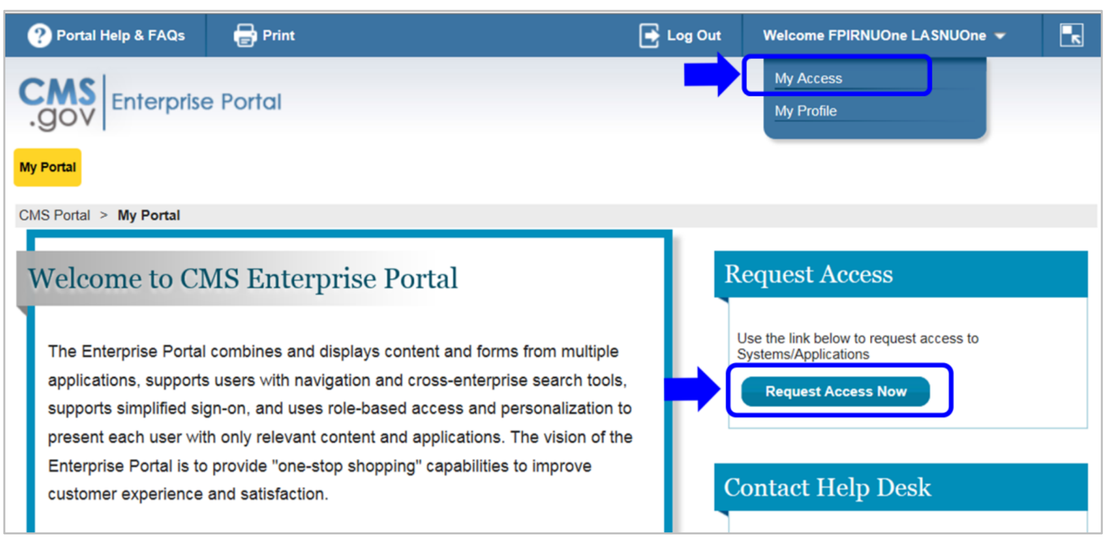
This section provides the following instructions:

1. How to search for a user
2. How to remove a role attribute
3. How to remove a role
4. How to remove multiple roles or attributes
5. How to use the “Export Results” feature

Searching 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	Log into the CMS Enterprise Portal. Select the down arrow icon that appears next to your name at the top of the page. Then, select **My Access** from the drop-down list to continue. Alternately, you may select **Request Access Now** to continue. **Note** After logging in, EIDM checks if you are an approver for one or more applications.



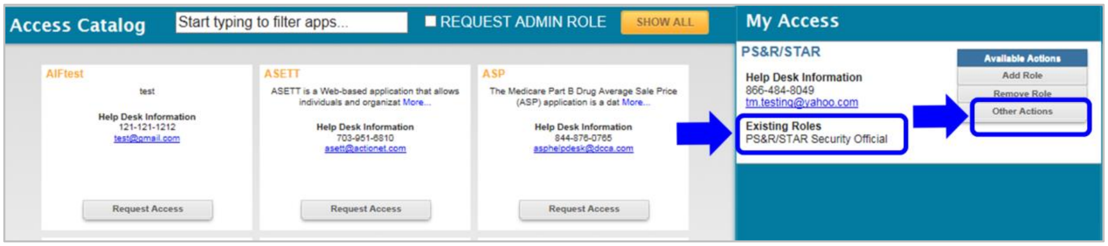
Action

Step 2

The **Access Catalog**, **My Access,** and **My Pending Requests** sections display.

The existing roles you have in each application display 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 displays.

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

Step 4

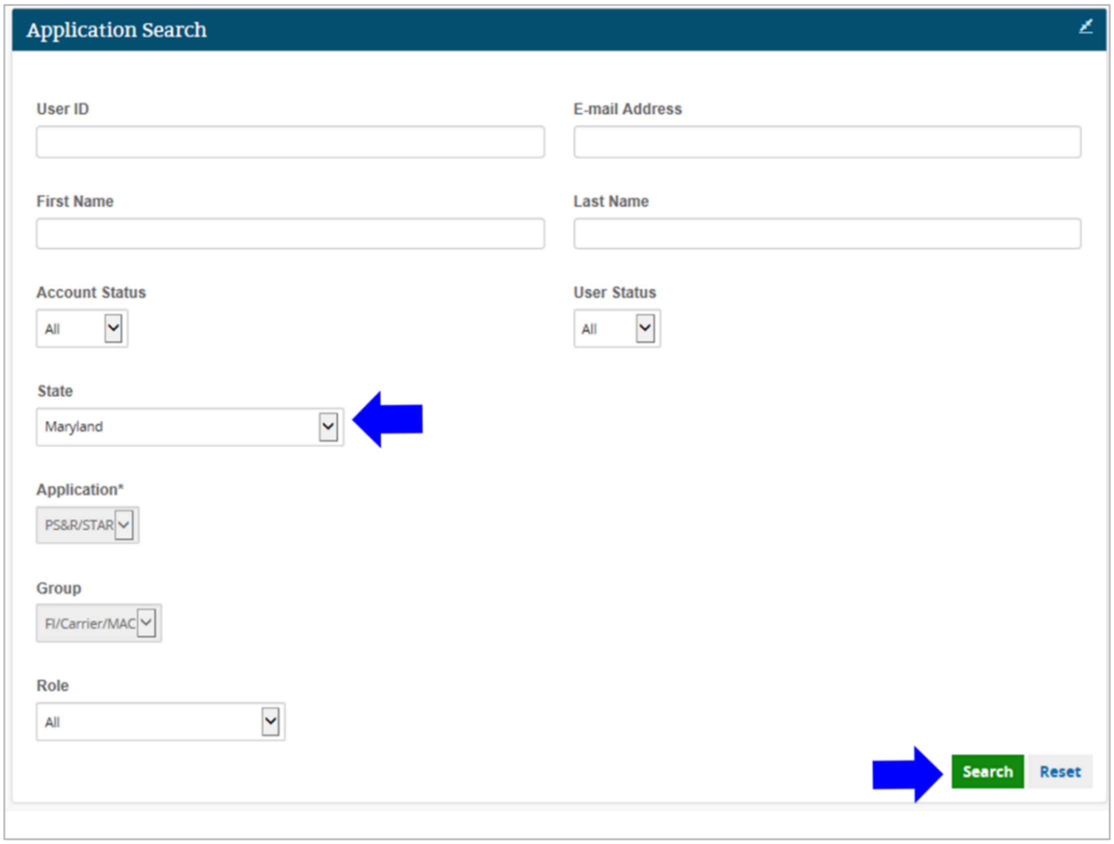
The **Application Search** page displays.

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’.

The user must enter a minimum of two (2) characters in the ‘User ID’, ‘First Name’, ‘Last Name’, or ‘E-mail’ fields if they are part of the search criteria.

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

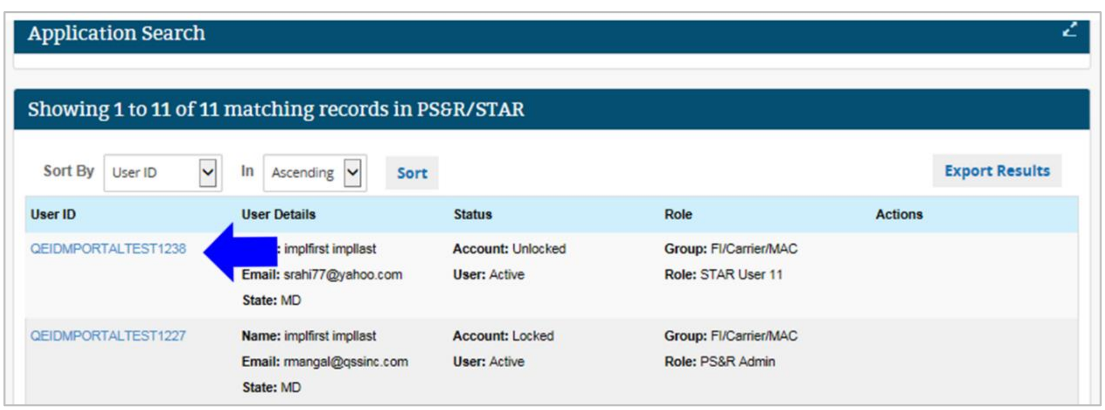
Action



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

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

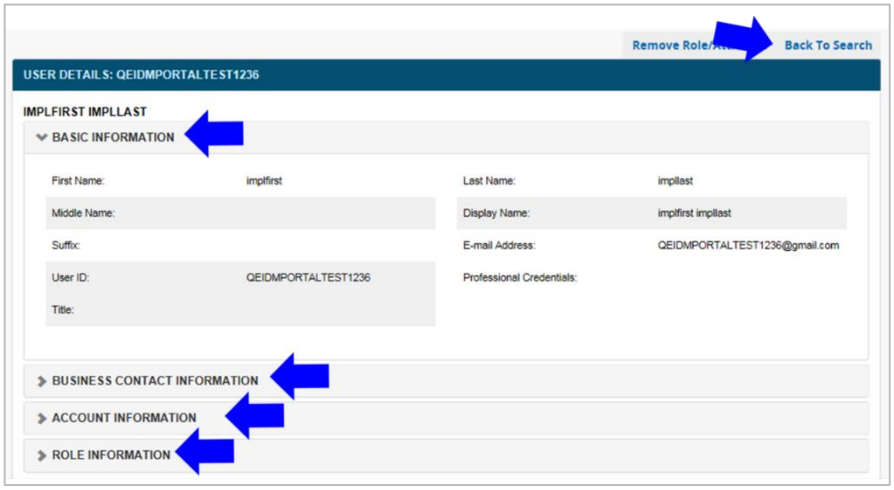
Note
You may select **Cancel** at any time to exit out of the "View and Manage Users" process. This action does not save any search information, user information, or changes.



	Action
Step 6	The **User Details** page displays.

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.



Removing Role Attributes

This section shows how to remove role attribute from a user's profile, if you have the authority. See Appendix B: 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

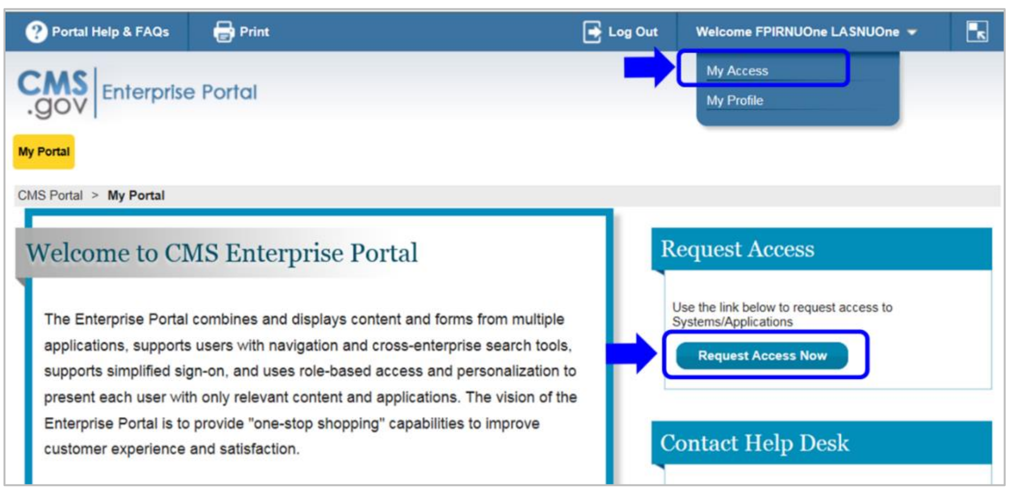
Step 1

Log into the CMS Enterprise Portal.

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

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

Note
After logging in, EIDM checks if you are an approver for one or more applications.

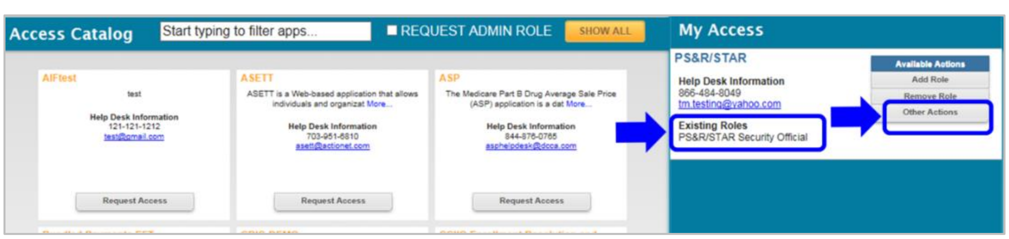


Step 2

The **Access Catalog**, **My Access,** and **My Pending Requests** sections display.

The existing roles you have in each application display 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 displays. Select **View and Manage Users** to continue.

Step 4

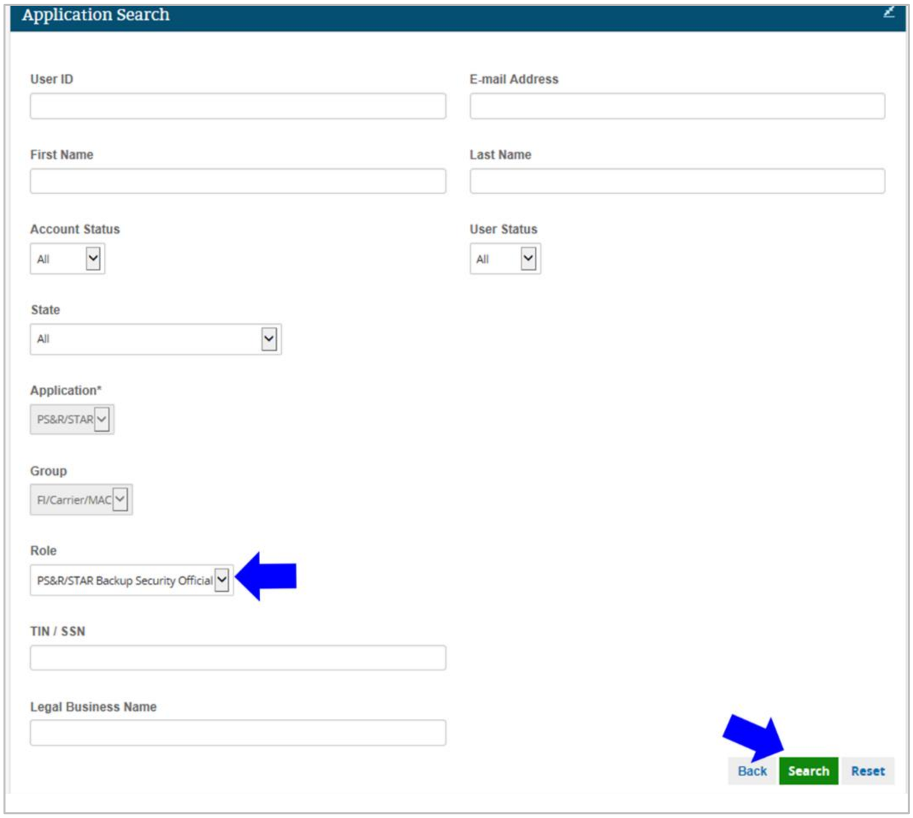
The **Application Search** page displays.

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

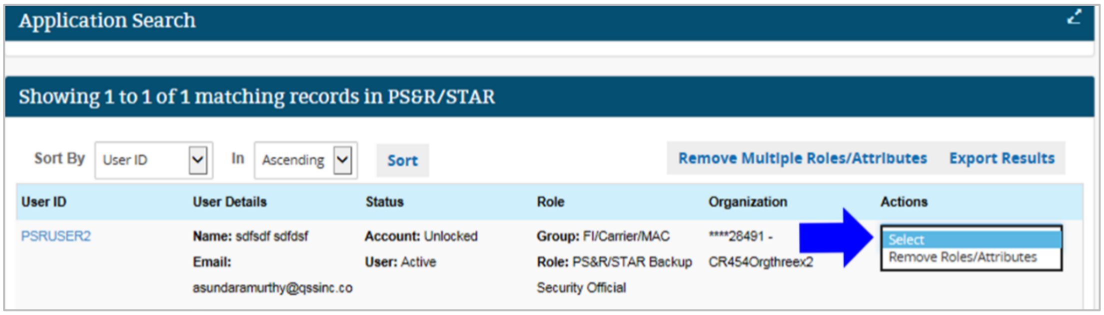
Step 5

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

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

Note

You may select **Cancel** at any time to exit out of the View and Manage Users process. This action does not save any search information, user information, or changes.

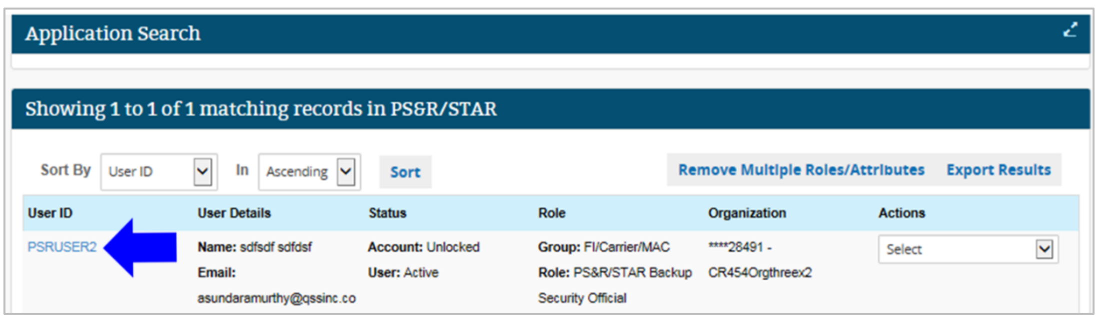


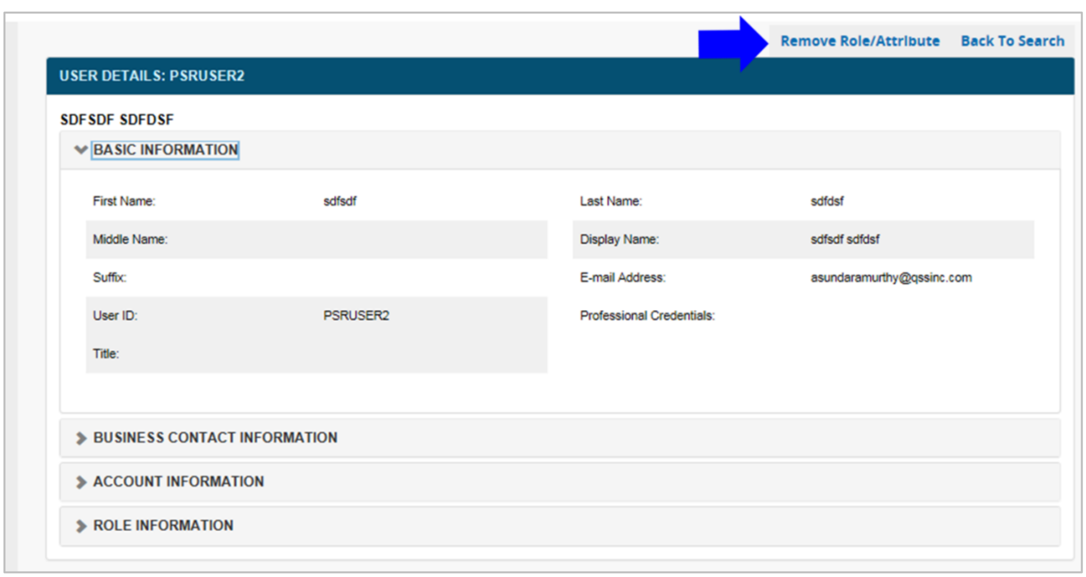
Step 6

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

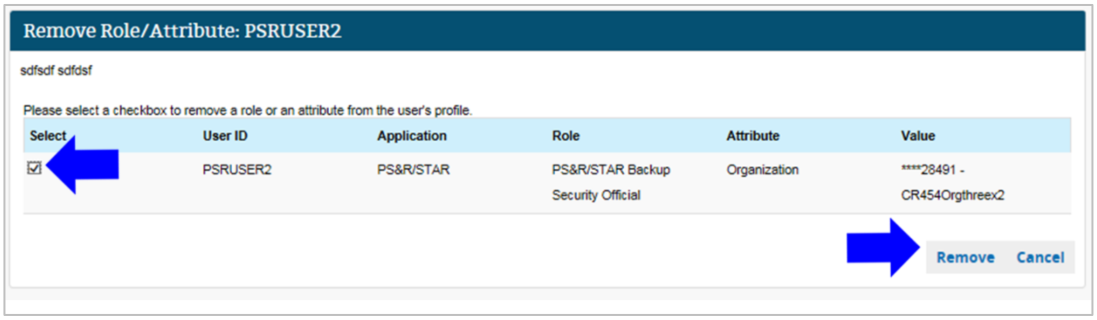
The **User Details** page displays.

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

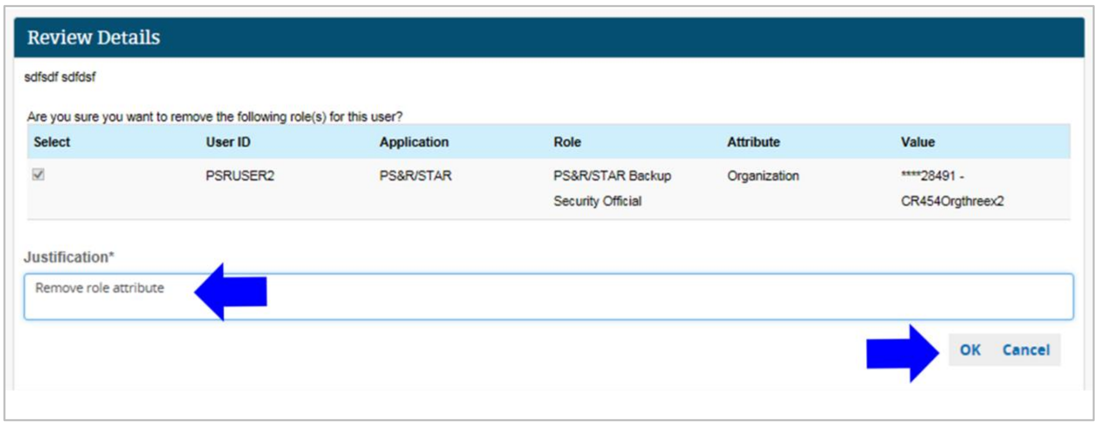




	Action
Step 7	The **RemoveRole/Attribute** page displays. Check the checkbox next to the attribute you want to remove. Select **Remove** to remove the attribute.



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



Step 9	An acknowledgement message displays. Select **OK** to return to the **Application Search** page.

Removing a Role

This section shows how to remove a call center from a person's role, if you have the authority. See Appendix B: 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

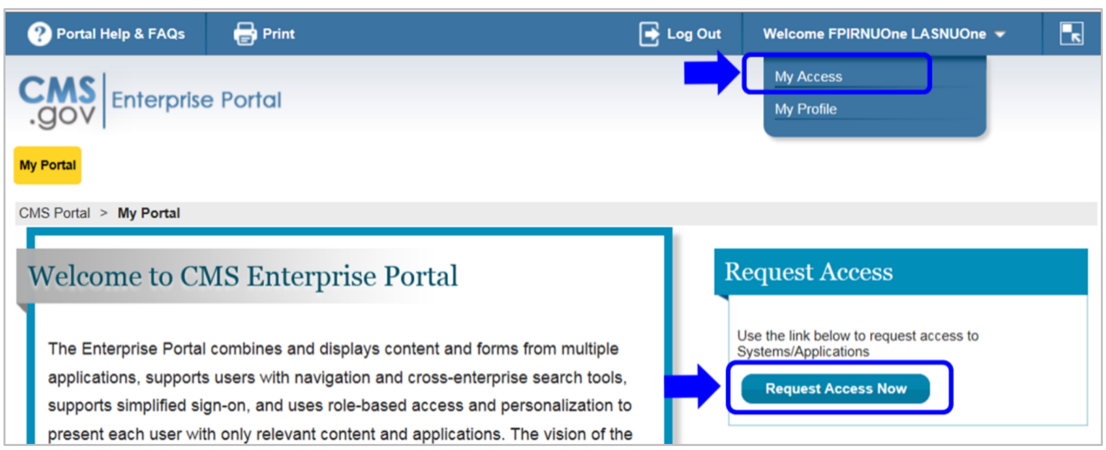
Step 1 Log into the CMS Enterprise Portal.

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

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

Note

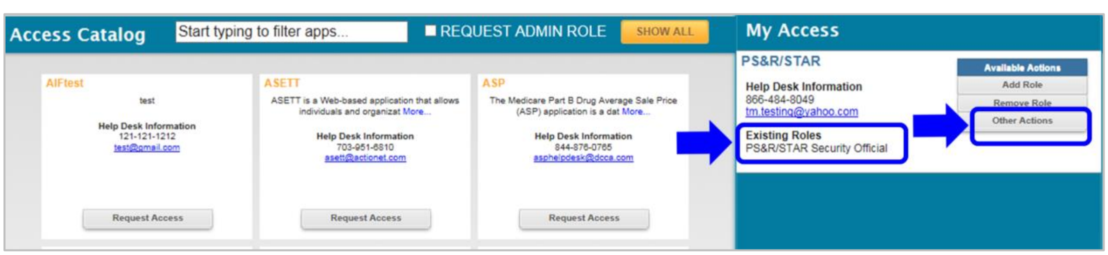
After logging in, EIDM checks if you are an approver for one or more applications.



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

The existing roles you have in each application display 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 displays.

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

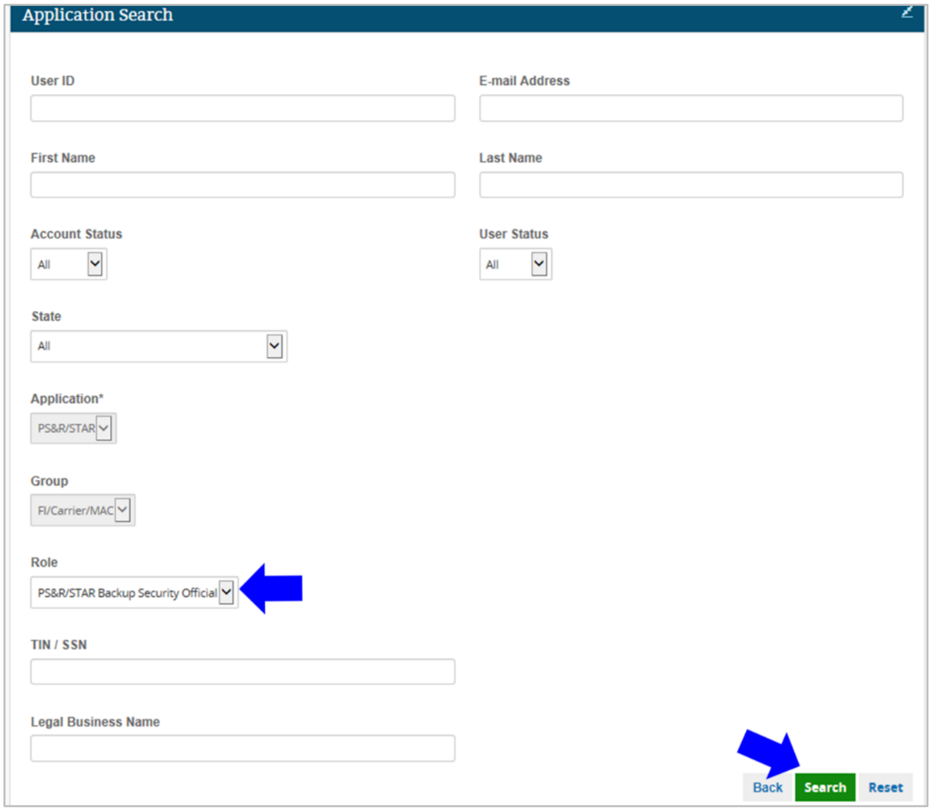
Step 4 The **Application Search** page displays.

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.

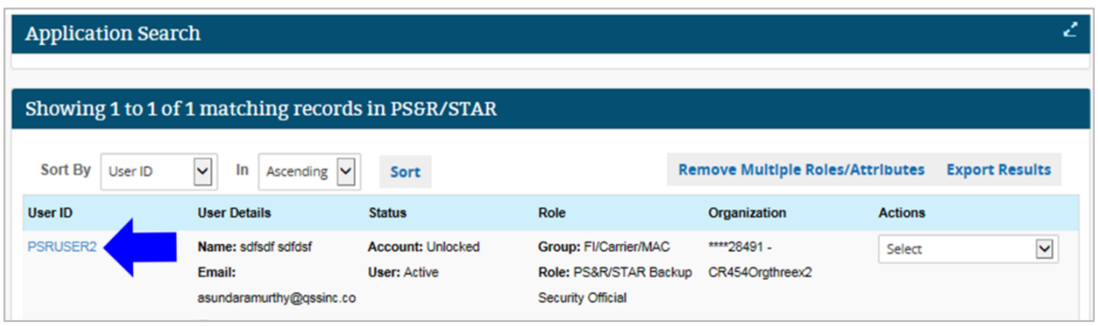
You must select a role in the search criteria for the 'Remove Roles/Attributes' option to be available on the results page***.***

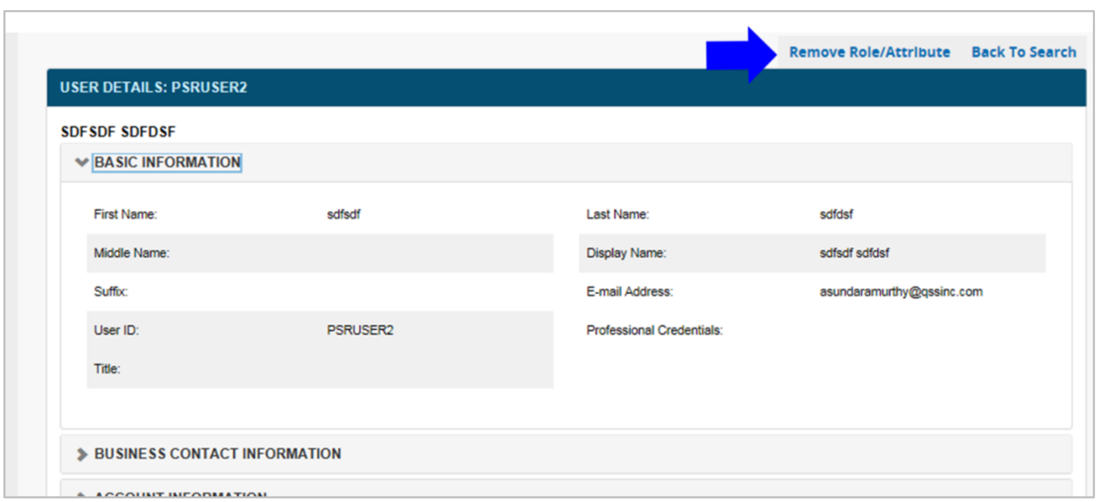
Provide the appropriate information to locate the individual or individuals needed and then select **Search**.



	Action
Step 5	After selecting **Search**, all of the persons in the application matching the search criteria, that you are authorized to view, display in the **Search Results** section. Under **Actions**, select **Remove Roles/Attributes** from the drop-down list. **Note** You may select **Cancel** at any time to exit out of the View and Manage Users process. This action does not save any search information, user information, or changes.

Step 6	Alternately, select the person's **User ID** to view the person's role information. The **User Details** page displays. Select **Remove Role/Attribute** at the top of the page.





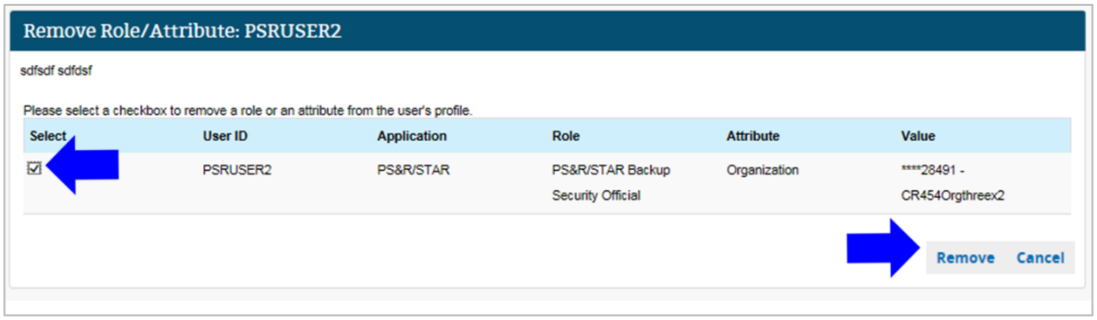
Action

Step 7 The **RemoveRole/Attribute** page displays.

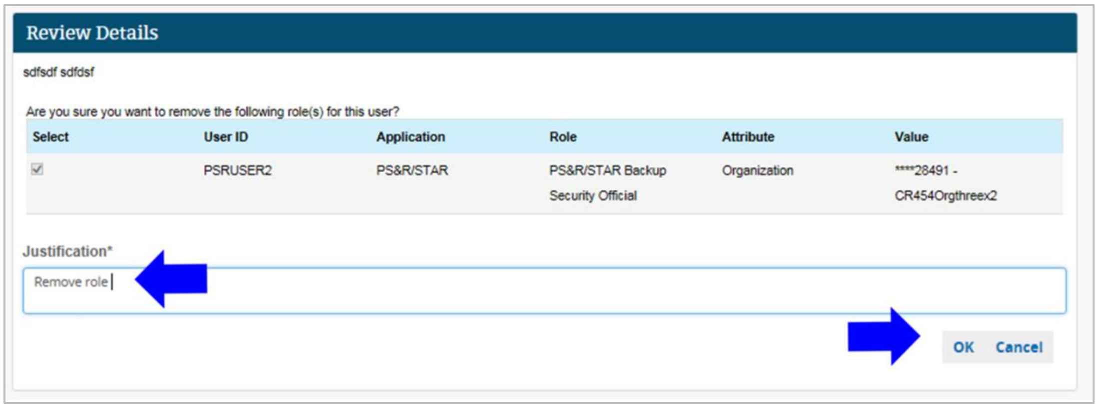
Select the check for the role you want to remove.

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**.



Step 9 An acknowledgement message displays.

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

Removing 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

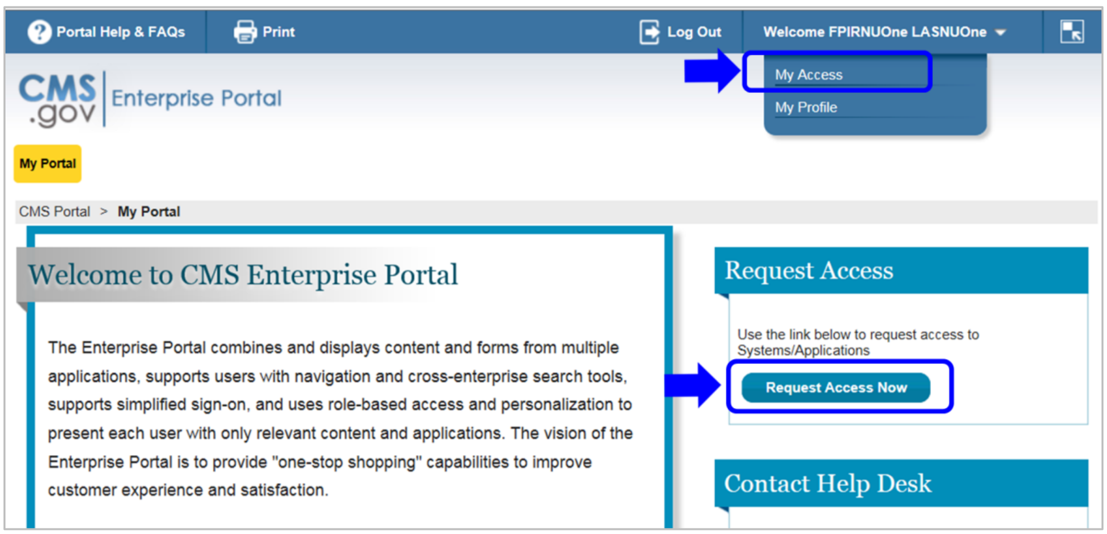
Step 1 Log into the CMS Enterprise Portal.

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

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

Note

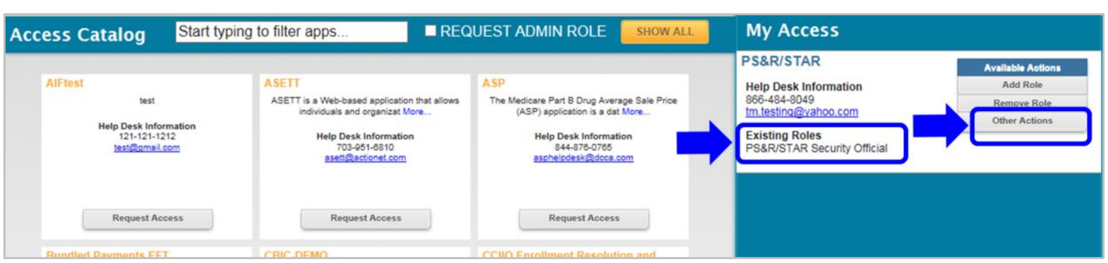
After logging in, EIDM checks if you are an approver for one or more applications.



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

Any existing roles you have in each application display 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.

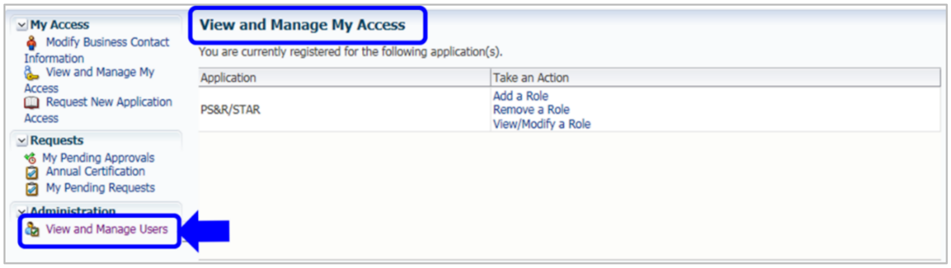


Action

Step 3

The **View and Manage My Access** page displays.

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



Step 4

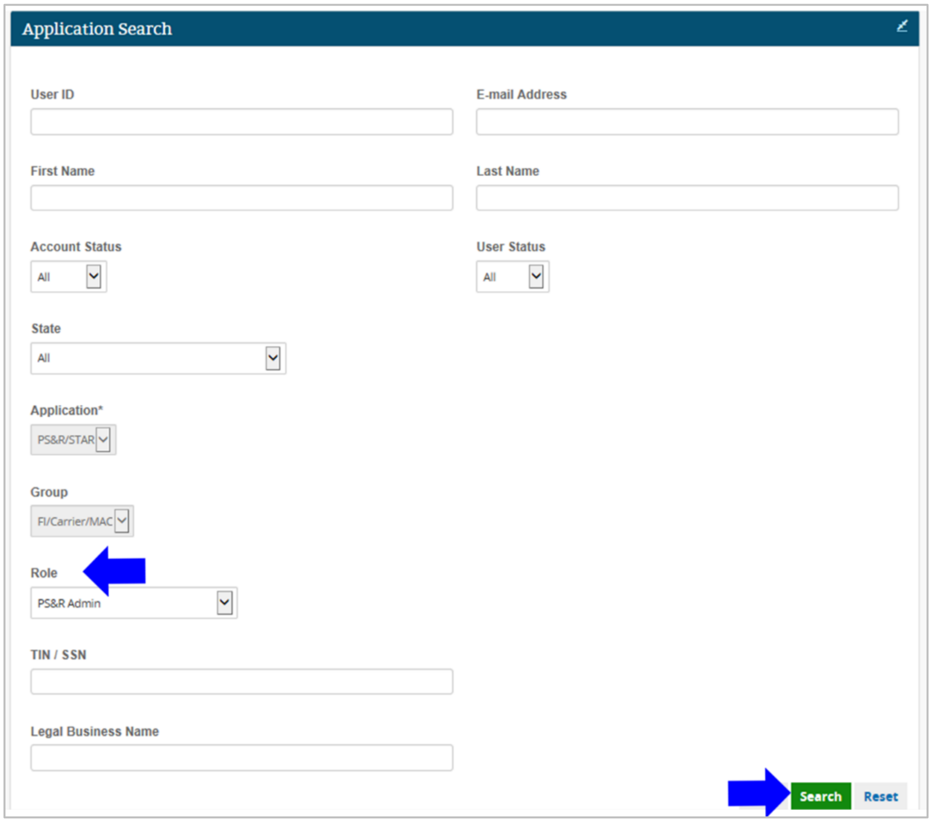
The **Application Search** page displays.

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’.

The user must enter a minimum of two (2) characters in the ‘User ID’, ‘First Name’, ‘Last Name’, or ‘E-mail’ fields if they are part of 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

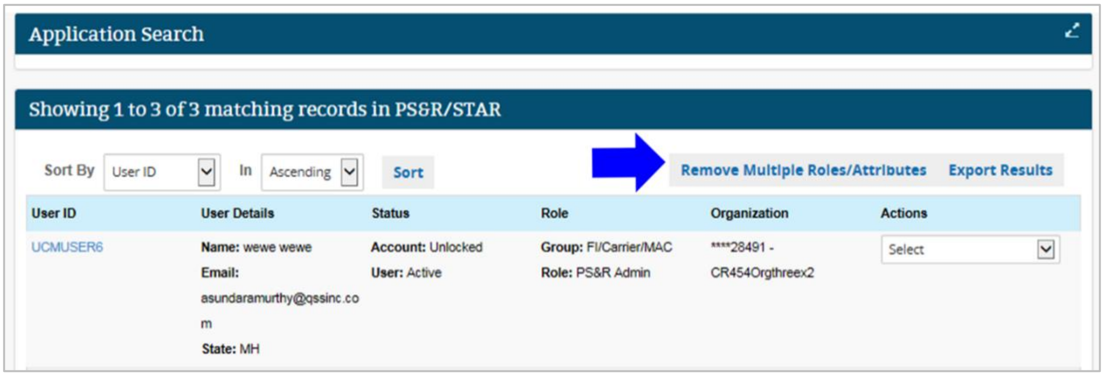
Step 5

After selecting **Search**, all of the persons in the application matching the search criteria, that you are authorized to view, display 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. This action does not save any search information, user information, or changes.



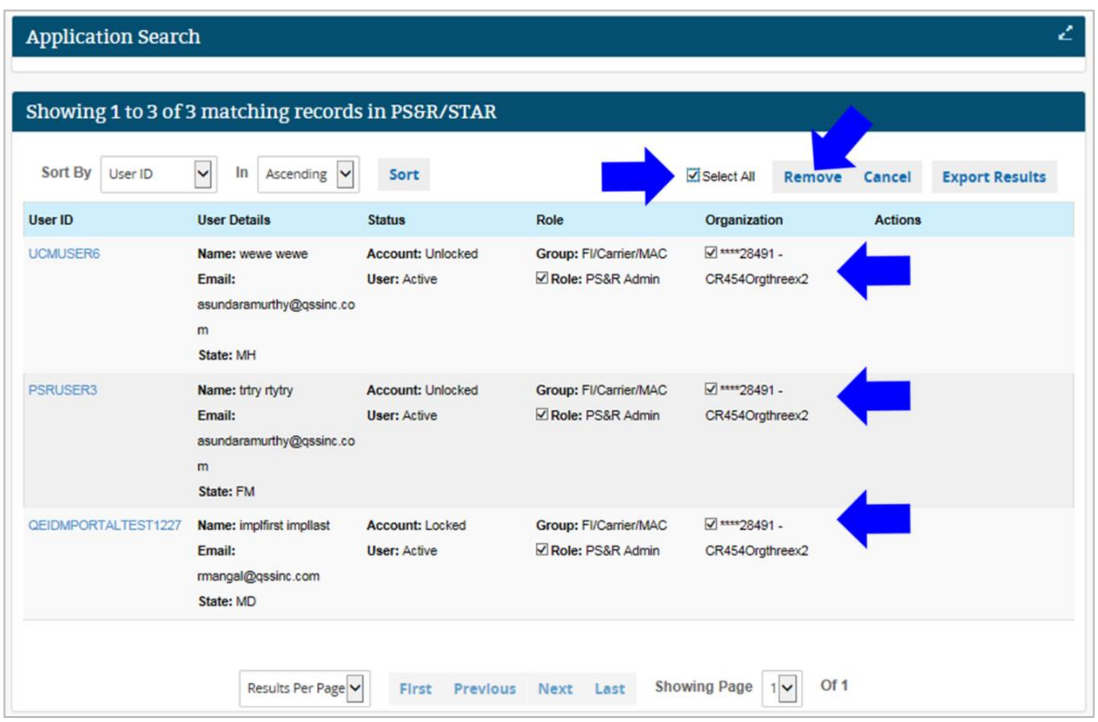
Step 6

The page updates to include checkboxes beside all roles and attributes. It also displays the **Select All** checkbox, **Remove** button, and **Cancel** button.

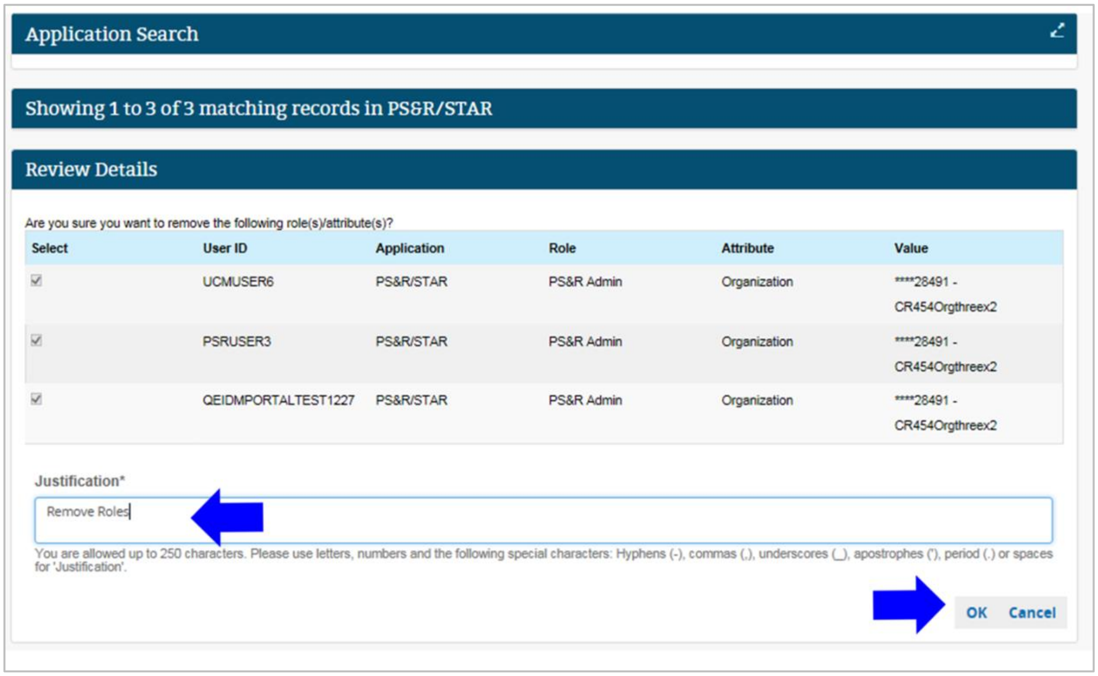
Check the boxes for the roles/attributes you want to remove and select **Remove**.

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	An acknowledgement message displays.
	Select **OK** to return to the **Application Search** page.

Exporting Results

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

Action

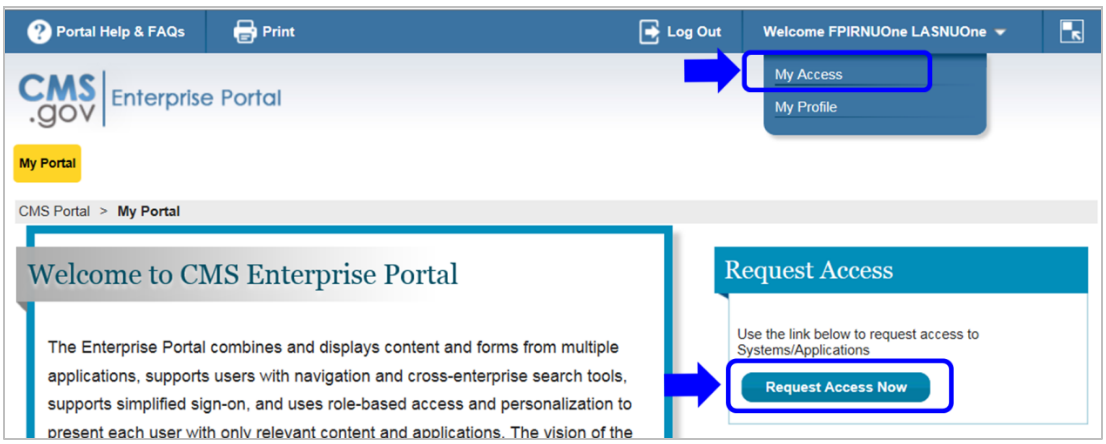
Step 1 Log into the CMS Enterprise Portal.

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

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

Note

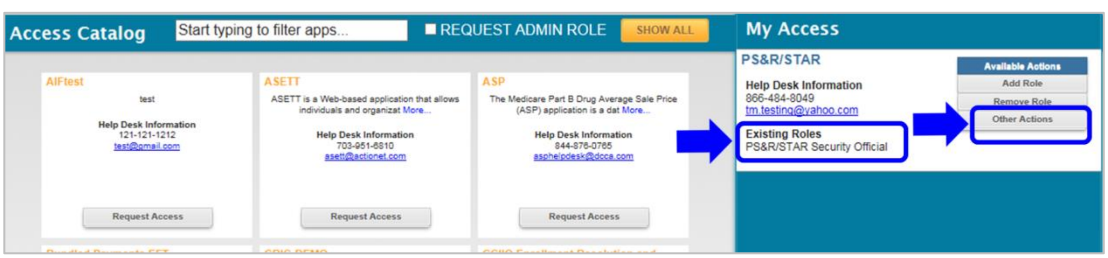
After logging in, EIDM checks if you are an approver for one or more applications.



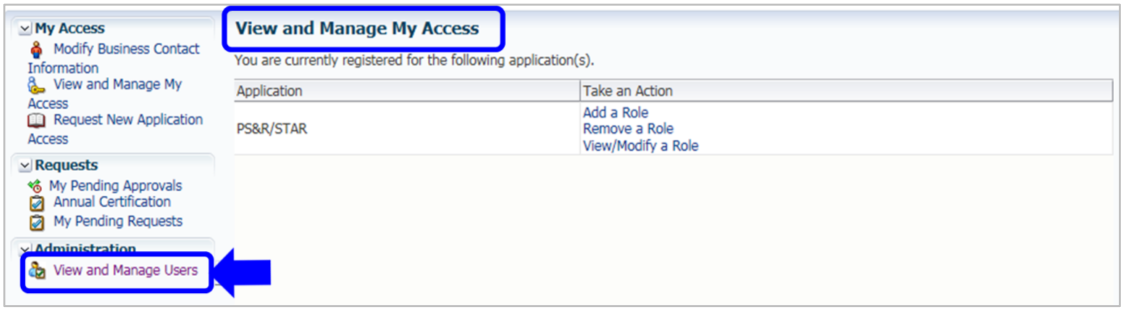
Step 2 The **Access Catalog**, **My Access,** and **My Pending Requests** sections display.

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

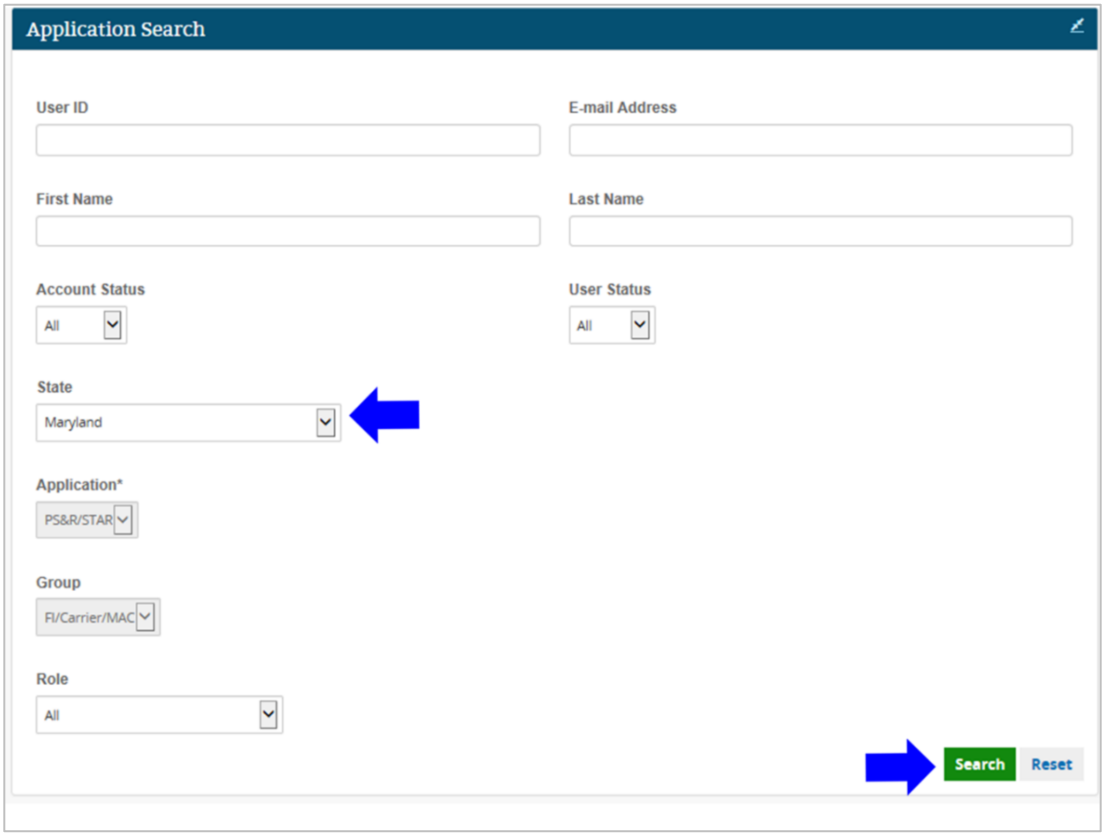
Select **Other Actions** in the **My Access** section to continue.



	Action
Step 3	The **View and Manage My Access** page displays. Select **View and Manage Users** to continue.



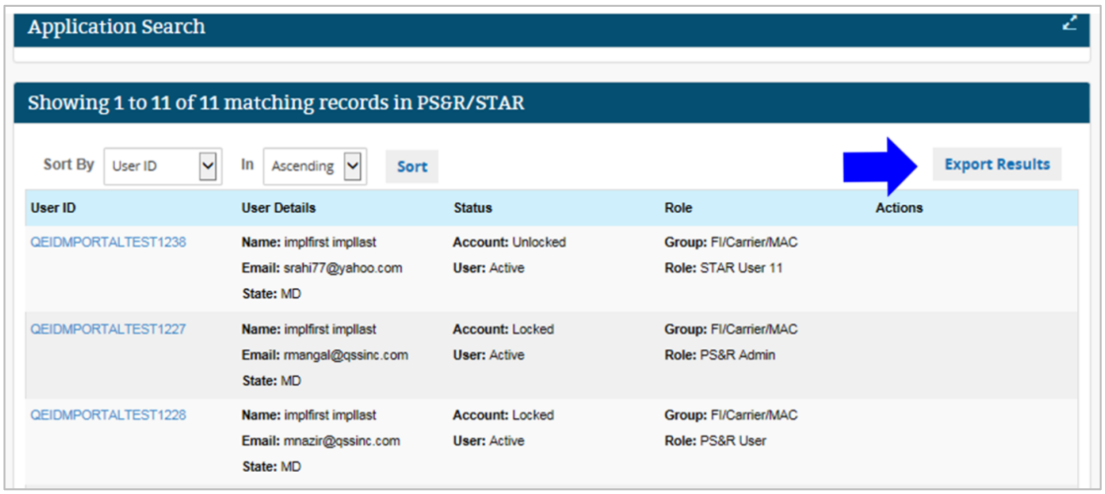
Step 4	The **Application Search** page displays. You may search for an individual, or individuals, by entering at least the Application as the search criteria or a combination of Application and any of the options such as ‘User ID’, ‘First Name’, ‘Last Name’, ‘E-mail Address’, ‘User Status’, ‘Account Status’, ‘State’, ‘Role’, and ‘Role Attributes’. The user must enter a minimum of two (2) characters in the ‘User ID’, ‘First Name’, ‘Last Name’, or ’E-mail’ fields if they are part of the search criteria. Provide the appropriate information to locate the individual or individuals needed and then select **Search**.



	Action
Step 5	After selecting **Search**, all of the users in the application matching the search criteria, that you are authorized to view, display in the **Search Results** section. Select the **Export Results** button. The search results export to an Excel workbook.

Notes

- The Export Results limit for the Application Search is 1,000 users.
- You may select **Cancel** at any time to exit out of the View and Manage Users process. This action does not save any search information, user information, or changes.



6. Appendices

Appendix A: 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

Application (Help Desk Name)	Phone	E-mail
FCSO aka The Spot *(FCSO Help Desk)*	855-416-4199	FCSOSpotHelp@FCSO.com
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

Application *(Help Desk Name)*	Phone	E-mail
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 *(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 2: Application Help Desk Information

Appendix B: Approver Roles and Functions

Application	Approver Role that can Remove Roles/Attributes	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

Table 3: Approver Roles and Functions

Appendix C: Acronyms

Acronym	Literal Translation
ACO	Accountable Care Organization
ASETT	Administrative Simplification Enforcement and Testing Tool
CBIC	Competitive Bidding Implementation Contractor
CC	Cost Contract
CERRS	Center for Consumer Information and Insurance Oversight (CCIIO) Enrollment Resolution and Reconciliation System
CGS	Celerian Group Administrators, LLC (collectively "CGS")
CHIP	Children's Health Insurance Program
CJR	Comprehensive Care for Joint Replacement
CMS	Centers for Medicare & Medicaid Services
COB	Coordination of Benefits
CPC	Comprehensive Primary Care
CPMS	Consumer Operated and Oriented Plan (CO-OP) Program Management System
CSR	Customer Service Representative
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies
ECRS	Electronic Correspondence Referral System
EFT	Electronic File transfer
EIDM	Enterprise Identity Management
ELMO	Eligibility and Enrollment Medicare Online
EPOC	External Point of Contact
EPPE	Enterprise Privacy Policy Engine
eRPT	Electronic Retroactive Processing Transmission
ESD	Enterprise System Development
FCSO	First Coast Service Options (The SPOT)
FFM	Federally-Facilitated Marketplace
FFSDCS	Fee for Service Data Collection System
GUI	Graphical User Interface
HDT	HIPAA Eligibility Transaction System (HETS) Desktop
HETS	HIPAA Eligibility Transaction System
HHVBP	Home Health Value-Based Purchasing
HIOS	Health Insurance Oversight System

Acronym	Literal Translation
HIPAA	Health Insurance Portability and Accountability Act
IC	Innovation Center
IVR	Interactive Voice Response
LBN	Legal Business Name
LOA	Level of Assurance
MA	Medicare Advantage
MACPro	Medicaid and CHIP Program
MAPD	Medicare Advantage - Prescription Drug
MARx	Medicare Advantage and Prescription Drug System
MCO	Medicaid Managed Care Organization
MCU	Marketplace Change Utility
MDR	Medicaid Drug Rebate
MED	Medicare Exclusion Database
MFA	Multi-Factor Authentication
MLMS	Marketplace Learning Management System
MMP	Medicare and Medicaid Plan
NPI	National Provider Identifier
PD	Prescription Drug
PDP	Prescription Drug Plan
PMDA	Medicaid 1115 Demonstrations Performance Metrics Database & Analytics System
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
PV	Physician Value
QMAT	Quality Measures Assessment Tool
SERTS	State Exchange Resource Tracking System
SERVIS	State Exchange Resource Virtual Information System
SHIP	State Health Insurance Assistance Program
SLS	Scalable Login System
SMS	Short Message Service

Acronym	Literal Translation
SSN	Social Security Number
STAR	System for Tracking Audit and Reimbursement
TIN	Taxpayer Identification Number
T-MSIS	Transformed—Medicaid Statistical Information System
UCM	Unified Case Manager
UI	User Interface
UID	User Identifier
VMS	Viable Information Processing Systems (ViPS) Medicare System
zONE	Opportunity to Network and Engage

Table 4: Acronyms