CMS Enterprise Identity Management (EIDM)

User Guide

Working Copy Version 0.4 Release 16 Final

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

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

Revision: May 2017

This page is intentionally blank.

Table of Contents

List of Tables

EIDM User Guide

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) is a federal agency that ensures health care coverage for more than 100 million Americans. CMS administers Medicare and provides funds and guidance for all of the 50 states in the nation, for their Medicaid programs and Children's Health Insurance Program (CHIP). CMS works together with the CMS community and organizations in delivering improved and better coordinated care.

What is EIDM?

CMS has established the Enterprise Identity Management (EIDM) 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"?

This EIDM User Guide provides step-by-step instructions on how to register in EIDM, how to obtain access to an application and request a role, and how to manage your user profile.

2. Before You Begin

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

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

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

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

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

As part of getting started, please review the following procedures:

1. How to verify your Computer Settings.
2. What you may need before you begin.

If needed, please refer to Appendix A: Accessing 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**. **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**.

	Action
Step 3	Disable you browser's pop-up blockers. **Internet Explorer 11:** Open your browser, select the **Tools** icon, select **Internet options, open the Privacy tab**, uncheck the **Turn on Pop-up blocker** checkbox, and select **OK**. **Firefox:** Open your browser, select the **Menu** icon, select **Content** in the navigation pane, find the **Pop-ups** section, and uncheck the **Block Pop-up windows** checkbox. **Chrome:** Open your browser, select the **Menu** icon, select **Settings**, select **Show Advanced Settings**, find the **Privacy** section, select **Content Settings**, find the **Pop-Ups** section, select **Allow all sites to show pop-ups**, and select **Done**. **Safari:** Open your browser, select the **Safari** button, select **Preferences**, open the **Security** tab, find the **Web content** section, and uncheck the **Block pop-up windows** checkbox.

What You May Need Before You Begin

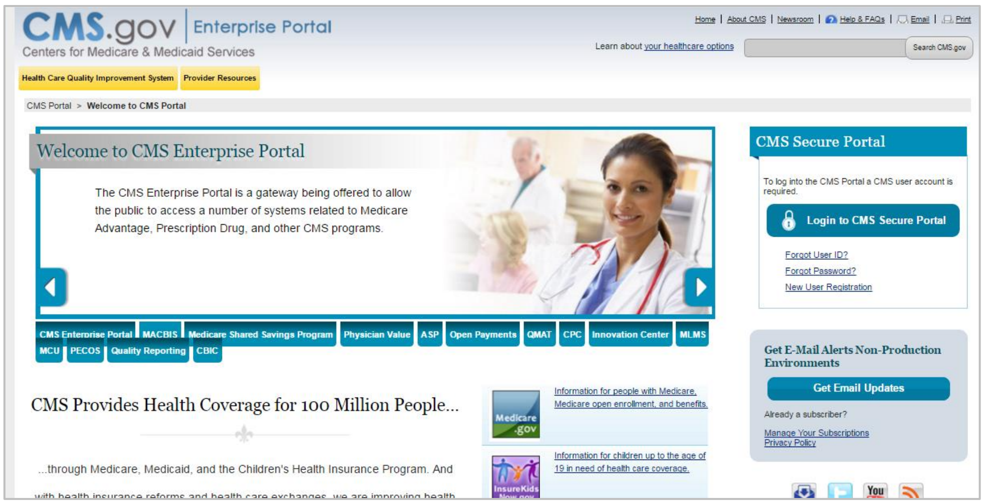
Prior to requesting access, you should have received instructions from your organization or CMS contact. They should include application-specific information you may need to complete the request, such as:

- 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.

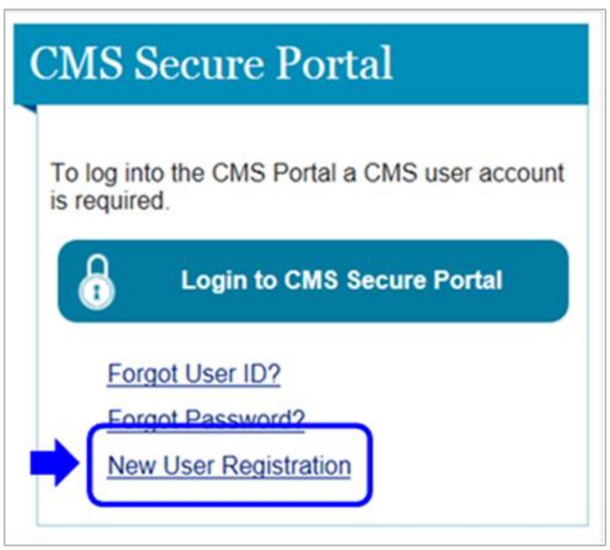
3. Registering for the Portal

This section provides information on how to register and create a user ID and password. The following are the basic step-by-step instructions.

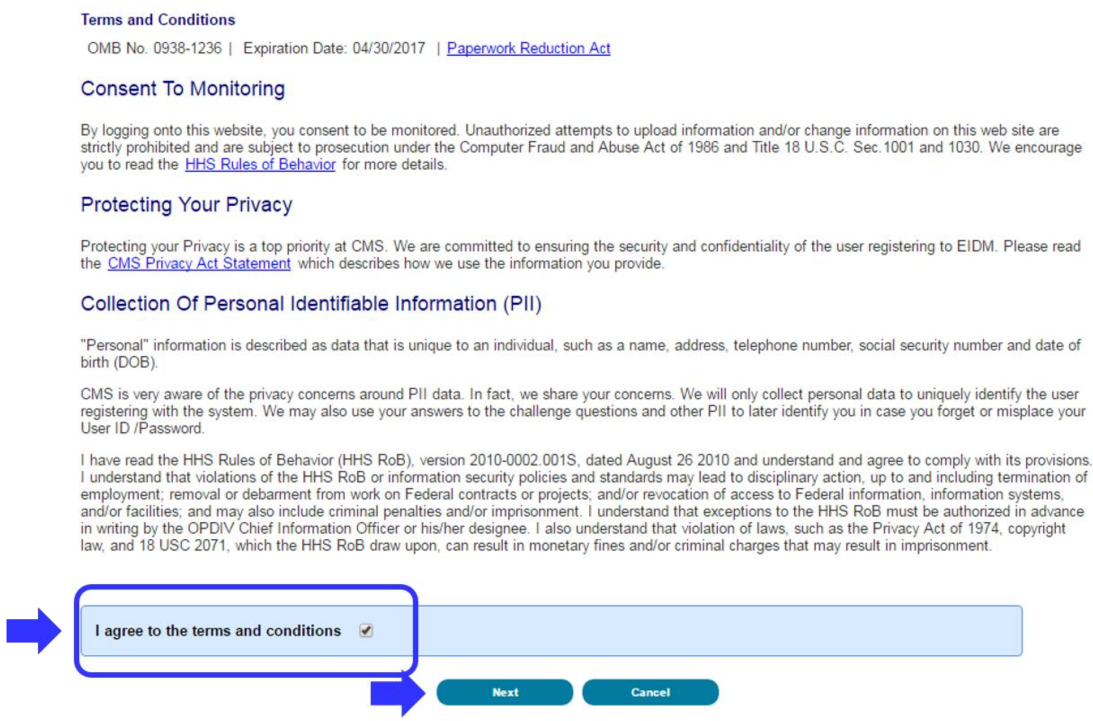
	Action
Step 1	Navigate to https://portal.cms.gov. The **CMS Enterprise Portal** page displays as illustrated below.



Step 2	Select the **New User Registration** link.



	Action
Step 3	Read the **Terms and Conditions**, select **I agree to the terms and conditions**, and then select **Next** to continue with the registration process.



Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 | Paperwork Reduction Act

Consent To Monitoring

By logging onto this website, you consent to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec.1001 and 1030. We encourage you to read the HHS Rules of Behavior for more details.

Protecting Your Privacy

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement which describes how we use the information you provide.

Collection Of Personal Identifiable Information (PII)

"Personal" information is described as data that is unique to an individual, such as a name, address, telephone number, social security number and date of birth (DOB).

CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal data to uniquely identify the user registering with the system. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

I have read the HHS Rules of Behavior (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

I agree to the terms and conditions

Next

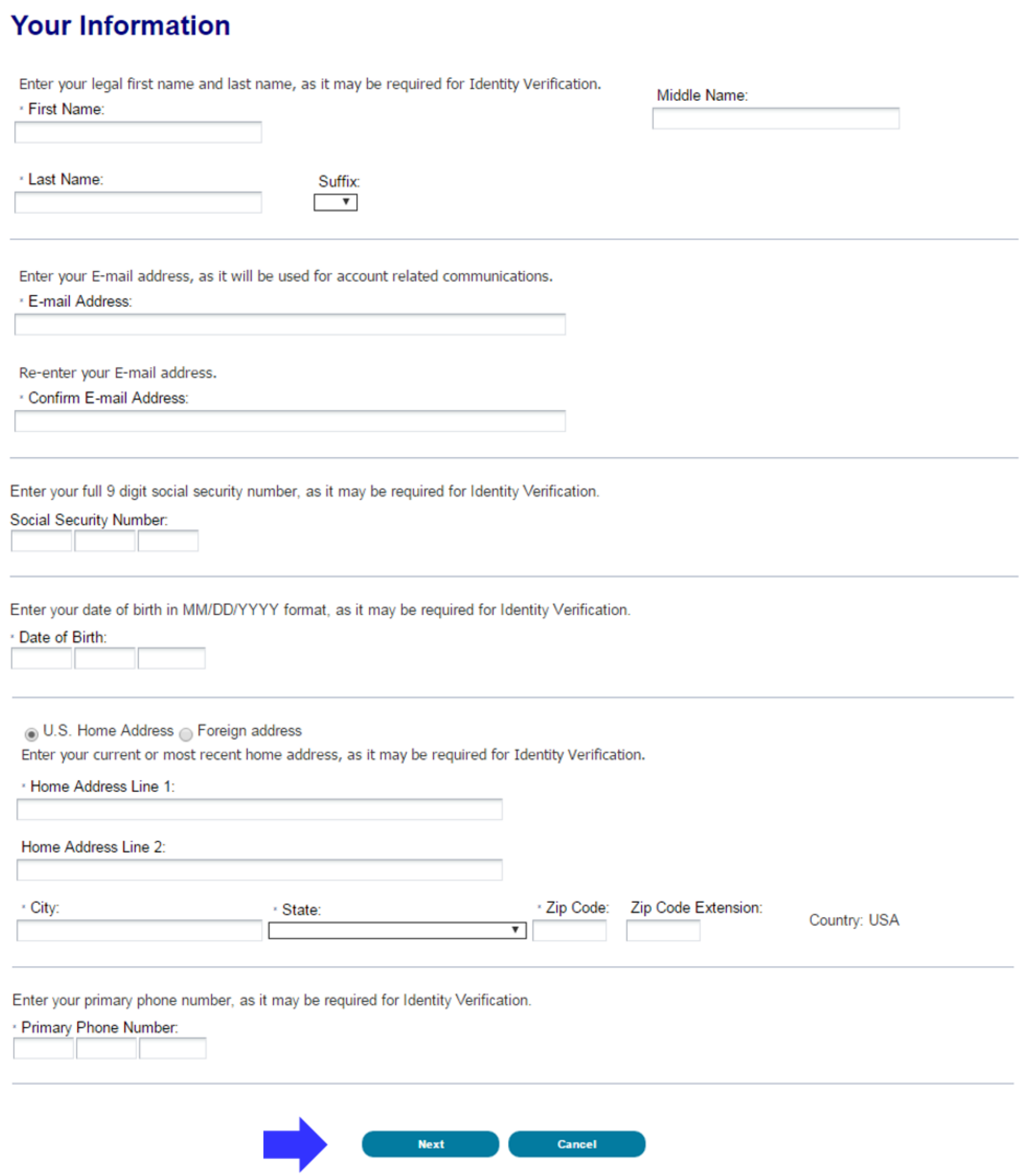
Cancel

	Action
Step 4	The **Your Information** page displays.

Provide the information requested on the **Your Information** page. The fields with an asterisk (*) are required fields and have to be completed.

After all required information has been provided, select **Next** to continue.

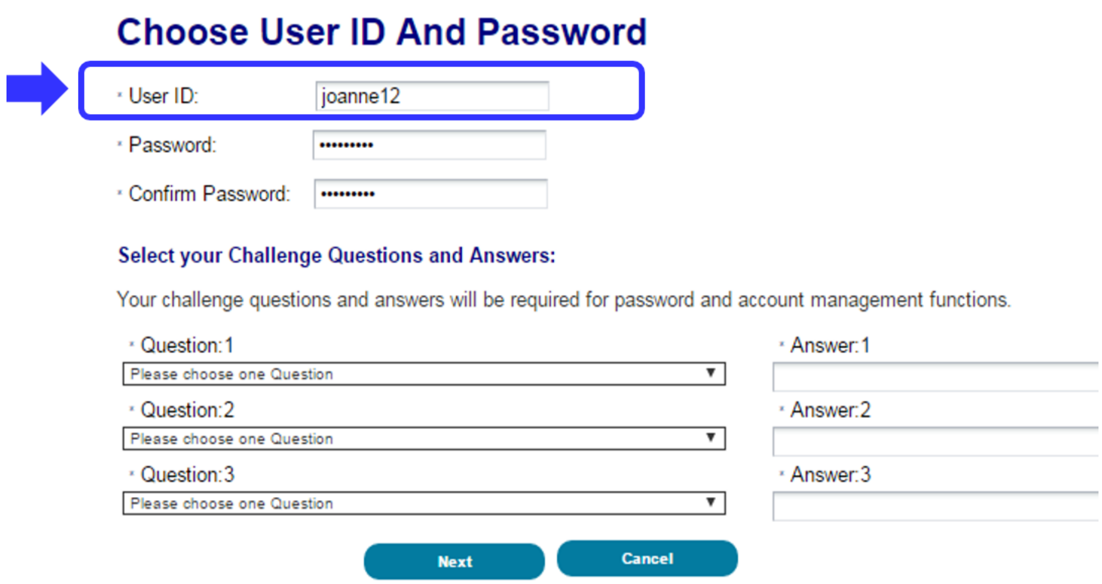
Note
You may select **Cancel** at any time to exit out of the registration process. New information or changes entered do not save.



Step	Action
Step 5	After providing the required information on the **Your Information** page, the **Choose User ID and Password** page displays. Create and enter a user ID of your choice, based on the requirements for creating a user ID.

Note

EIDM displays instructions on what you are required to include in your user ID.

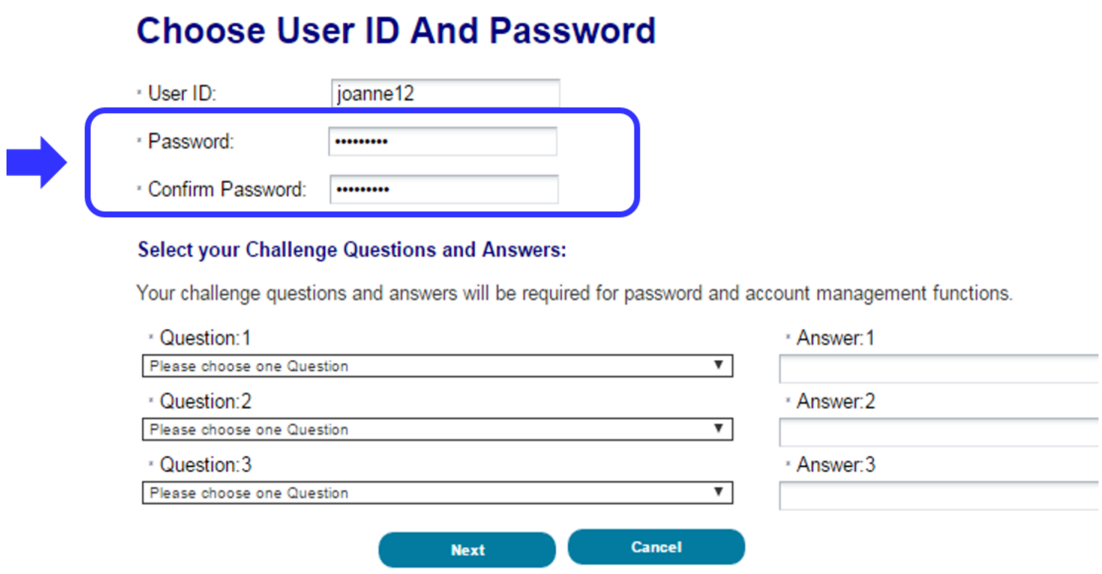


Step	Action
Step 6	Create and enter a password of your choice. Enter the same password in the **Confirm Password** field.

Notes

- EIDM displays instructions on what you are required to include in your password.
- Passwords must not contain any commonly used words or phrases that are 3 characters or more in length, such as “love”, “June”, “123”, etc.
- The passwords must match before you can continue.

Action


Choose User ID And Password
User ID:
joanne12
Password:
Confirm Password:
Select your Challenge Questions and Answers:
Your challenge questions and answers will be required for password and account management functions.
Question:1
Please choose one Question
Answer:1
Question:2
Please choose one Question
Answer:2
Question:3
Please choose one Question
Answer:3
Next
Cancel

Action

Step 7

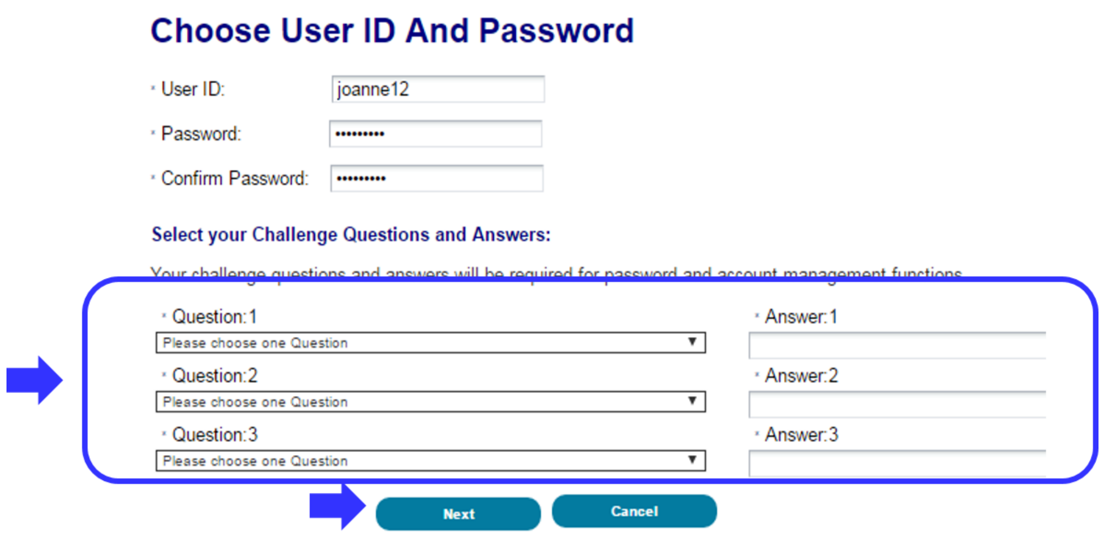
After entering the user ID and password you have created, select a question of your choice in the **Select your Challenge Questions and Answers** section and enter the answer you want to be saved with the question.

Continue to select a question and enter an answer for Question 2 and Question 3.

Select **Next** to complete the registration process.

Note

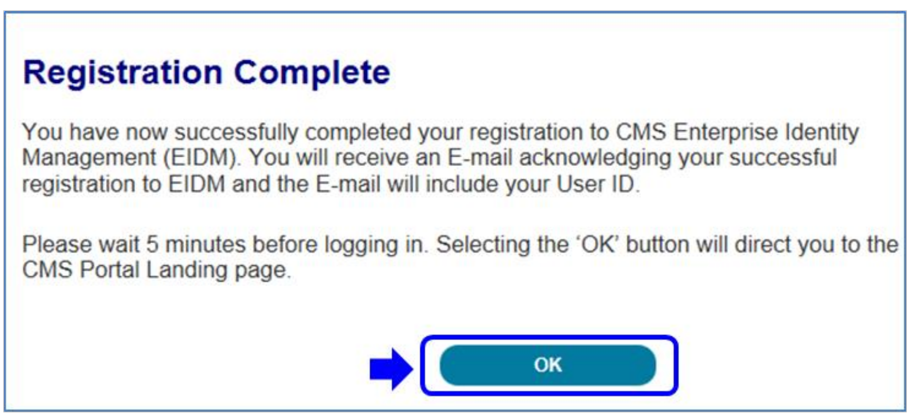
You may select **Cancel** to exit out of the registration process. New information or changes entered do not save.



Step 8

The **Registration Complete** page displays and informs you that you should receive an e-mail that acknowledges your successful registration and includes your user ID.

Select **OK** to close the **Registration Complete** page.



4. Logging In

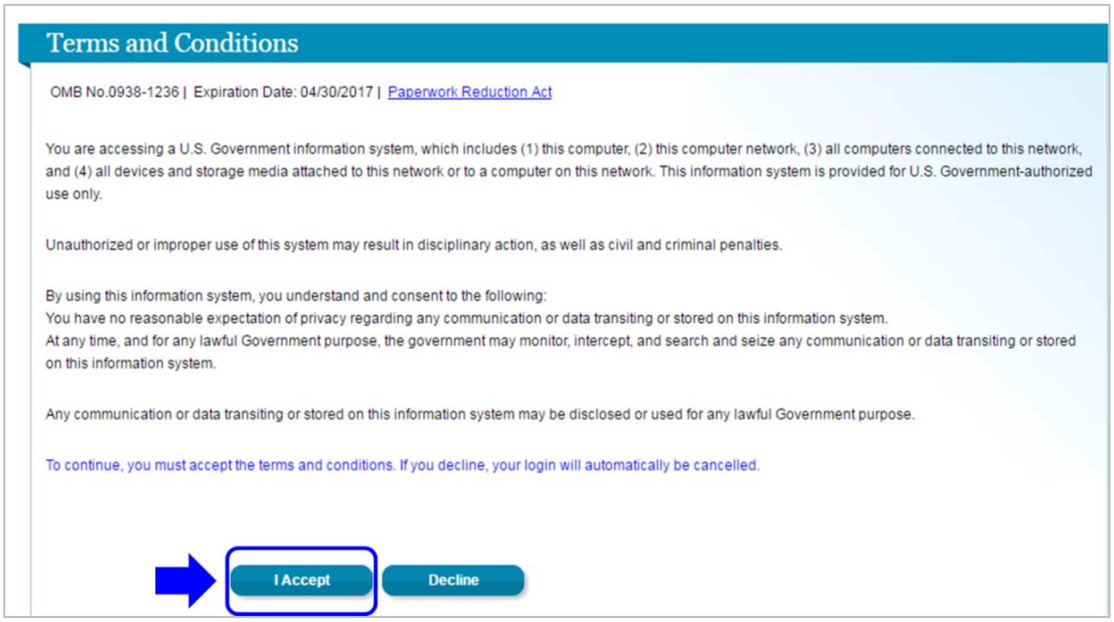
This section provides information on how to Login using your user ID and password. The following are the basic step-by-step instructions.

Action

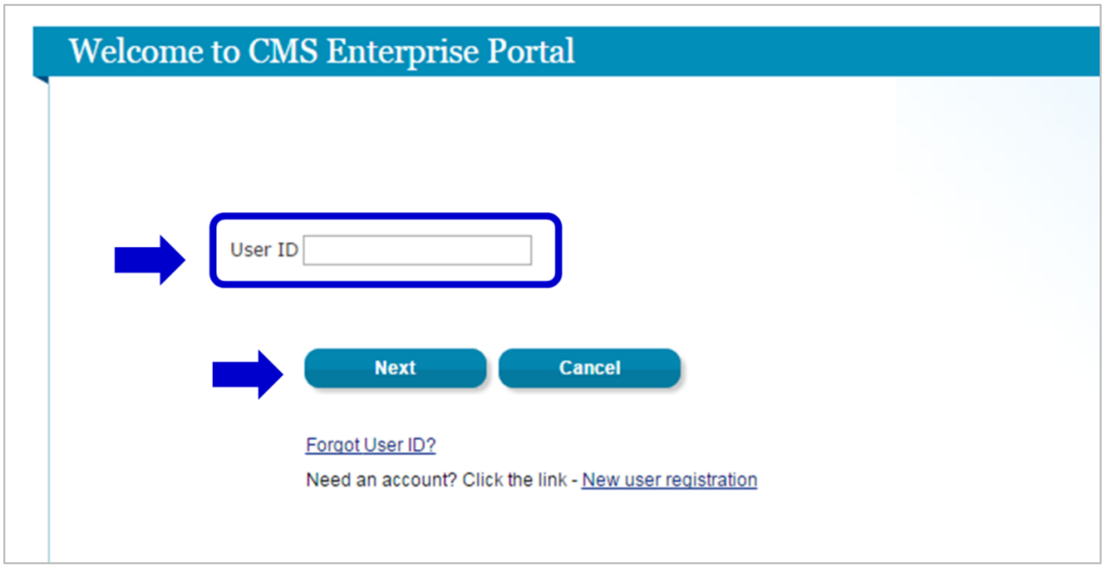
Step 1 Navigate to https://portal.cms.gov. The **CMS Enterprise Portal** page displays as illustrated below.

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

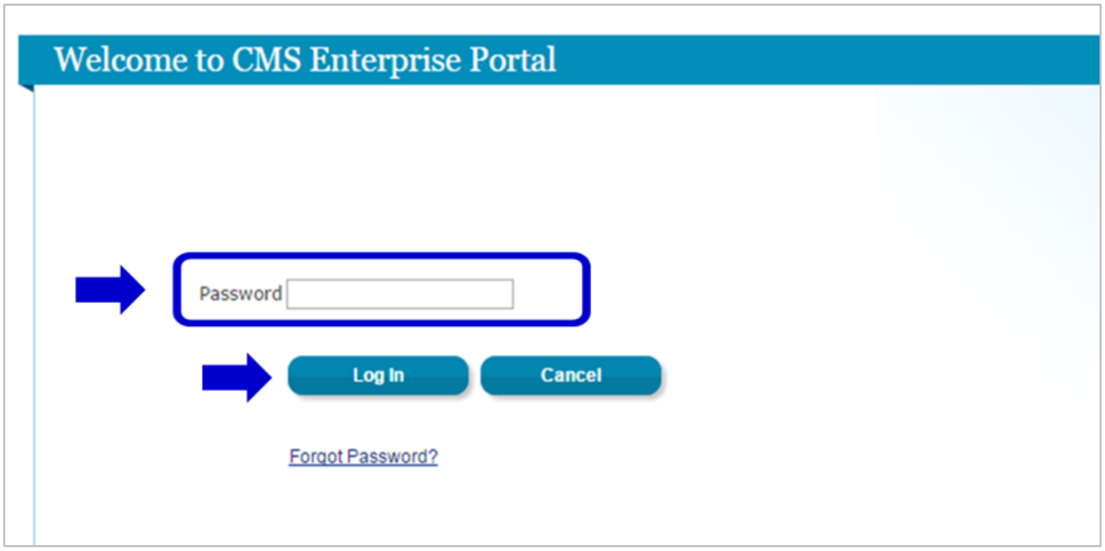
	Action
Step 3	Read the **Terms and Conditions** and select **I Accept** to continue.



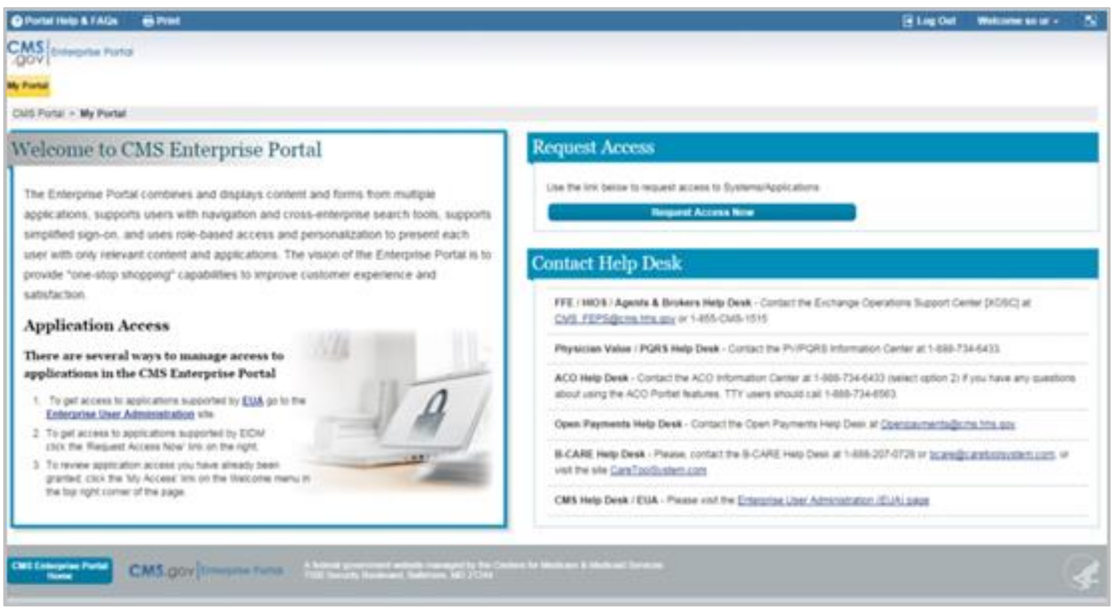
Step 4	Enter your **User ID** and select **Next** to continue.



	Action
Step 5	Enter your **Password** and select **Log In**.



Step 6	The system displays the **Welcome to CMS Enterprise Portal** page.



5. Requesting Access

This section provides basic step-by-step instructions and assistance on how to request access to an application and a role.

Note
If you do not have a user ID and password, you have to register and create a user ID and password. Please follow the steps under **How to Register and Create a User ID and Password**.

Each application is different and may require you to enter or select information not indicated in the basic step-by-step instructions in this User Guide.

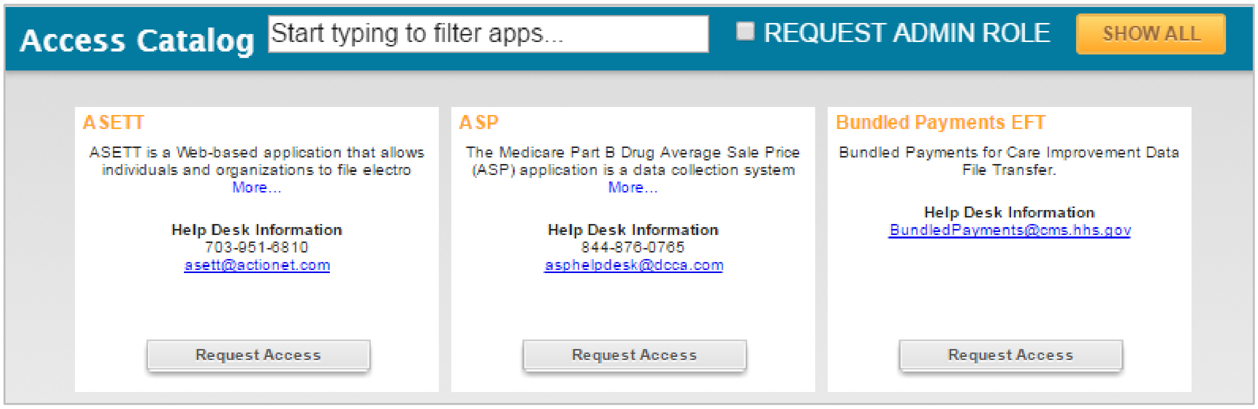
What if my application requires me to provide additional information that's not included in the basic step-by-step instructions?

After following the instructions for **How to Register and Create a User ID and Password**. EIDM prompts you to enter or select any additional information needed, based on the application and role you are requesting. In addition, EIDM displays help messages to assist you in completing your requests.

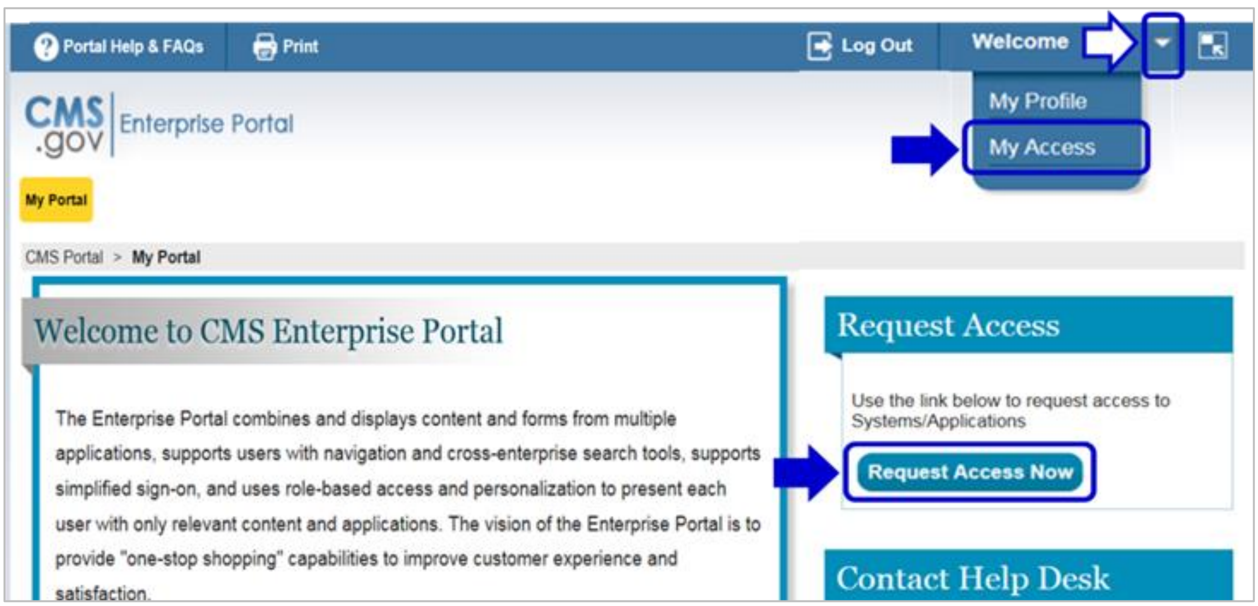
Note
If you currently have a role in an application and you need to request access for another role in the same application, please follow the step-by-step instructions for How to Add a Role

The Application Access Catalog

The application **Access Catalog** displays all the CMS applications that use EIDM services. Registered users who are logged into EIDM can use the catalog to request access to applications and select from a number of additional options that are described in more detail below.



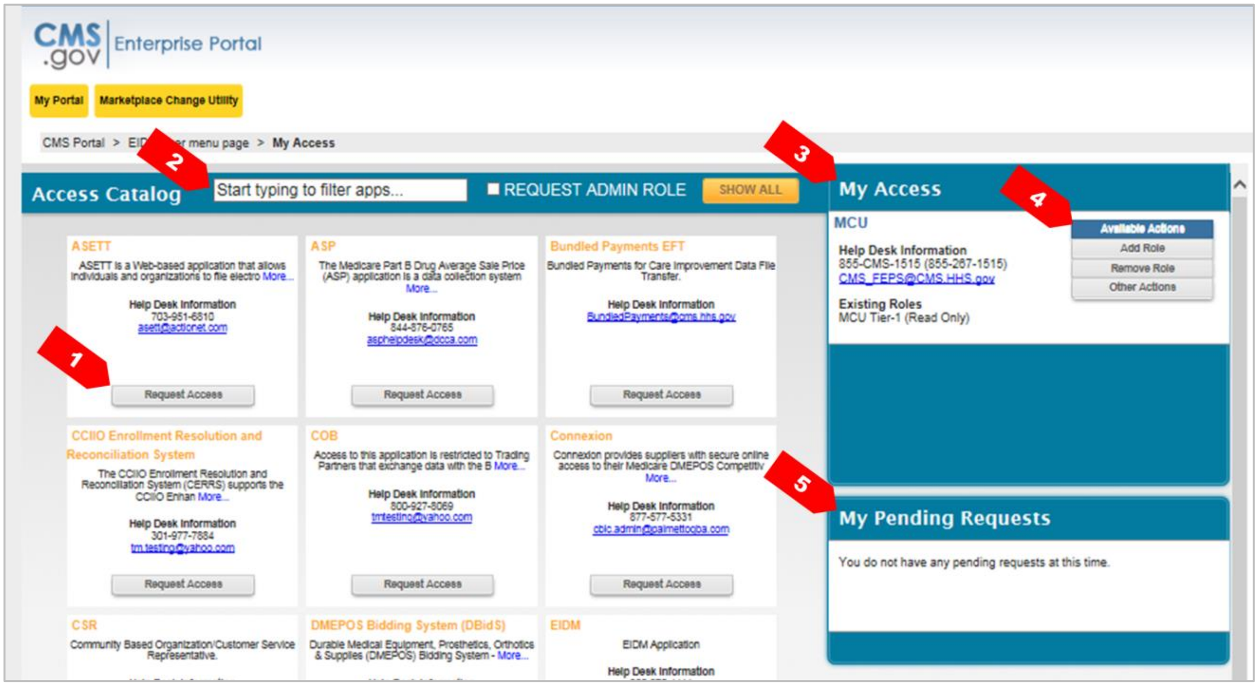
The catalog is accessed by selecting the **My Access** option from the CMS My Portal home page drop-down list or by selecting the **Request Access Now** button as shown in the image below. Requesting access is covered in more detail in the section titled **How to Request a Role**.



Access Catalog Features

The features listed below refer to the numbered image that follows.

1. **Request Access** – Request access to a particular application by selecting the **Request Access** button on the application's tile.
2. **Search** – Search for a particular application by typing the name of the application in the search box on the **Access Catalog** title bar.
3. **My Access** – This panel displays information for each application for which the user has access including:
    a. Contact information for the application's Help Desk.
    b. The existing roles the user has been granted for the application.
4. **Available Actions** – This panel appears for each application for which the user has access. The user can select from the following options:
    a. Add a Role – Directs the user to the **Request Additional Role** screen to request an additional role for the application.
    b. Remove a Role – Directs the user to the **View and Manage My Access** screen to remove a role from the application.
    c. Other Actions – Directs the user to the **View and Manage My Access** screen to select other options.
5. **My Pending Requests** – This section lists the pending requests for which the user has requested access.



How to Request a Role

The following are the basic step-by-step instructions on how to request access to an application and a role, when you currently do not have a role in the application.

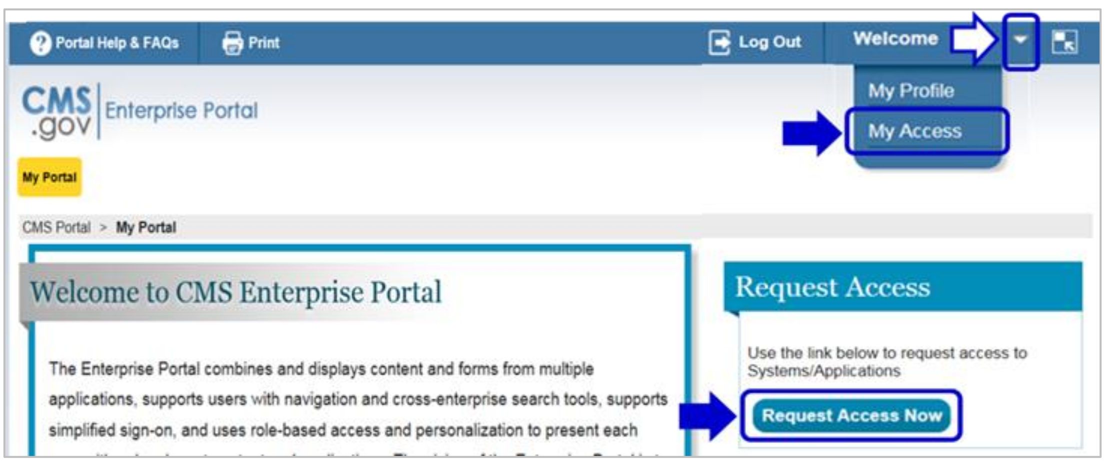
Important Note

To request a role for one of the applications listed below:

- ASETT
- ASP
- EPPE
- ESD
- FFM/Training– Agents/Brokers/Assisters
- IC
- IDHD
- MACPro
- MCU
- MLMS
- Open Payments
- SHIM
- T-MSIS
- zONE

To request a role 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.



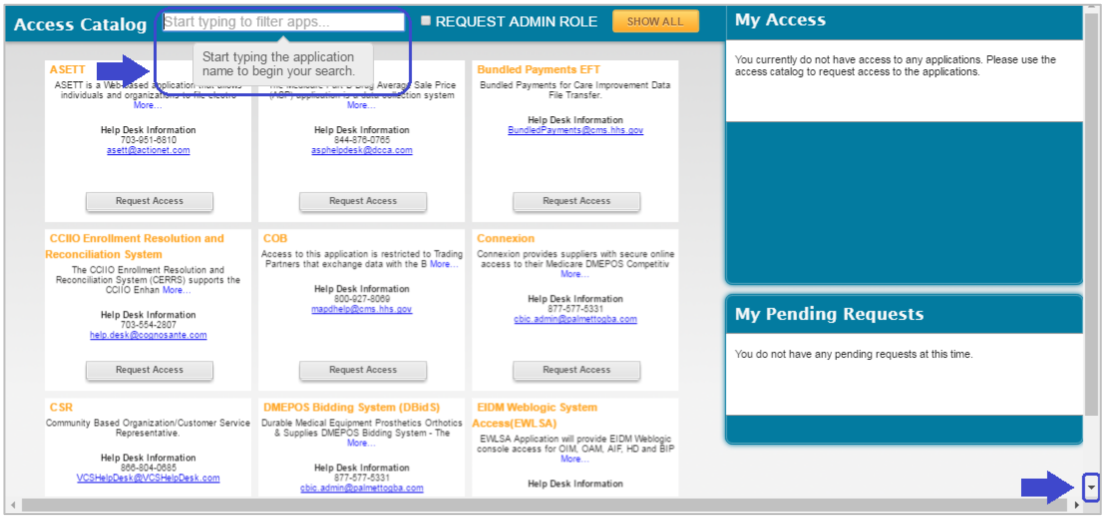
Action

Step2 The application **Access Catalog** displays.

Scroll down to locate the application you need.

Alternatively, enter the first few letters of the application in the **Search** section and all of the applications beginning with those letters display below.

> **Note**
>
> If you currently have access to one or more applications, they display in the **My Access** section. If you have pending requests, they display in the **My Pending Requests** section.



Step 3 After entering the first few letters of the application in **Search**, the applications beginning with those letters are displayed.

Select **Request Access** for the application you need.

Action

Step4 The **Application Description** and **Select a role** sections are displayed.

Select the role you need from the **Select a role** drop-down list.

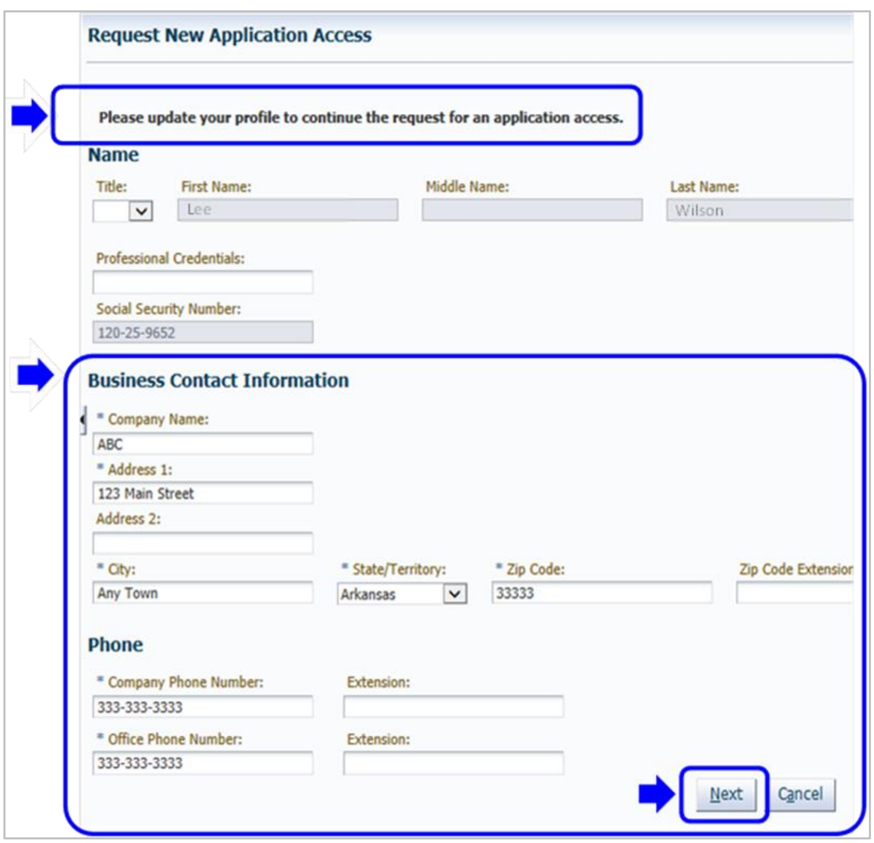
Step 5 The **Request New Application Access** page displays.

If all of your required business contact information is not on file, you have to provide this information before you can continue.

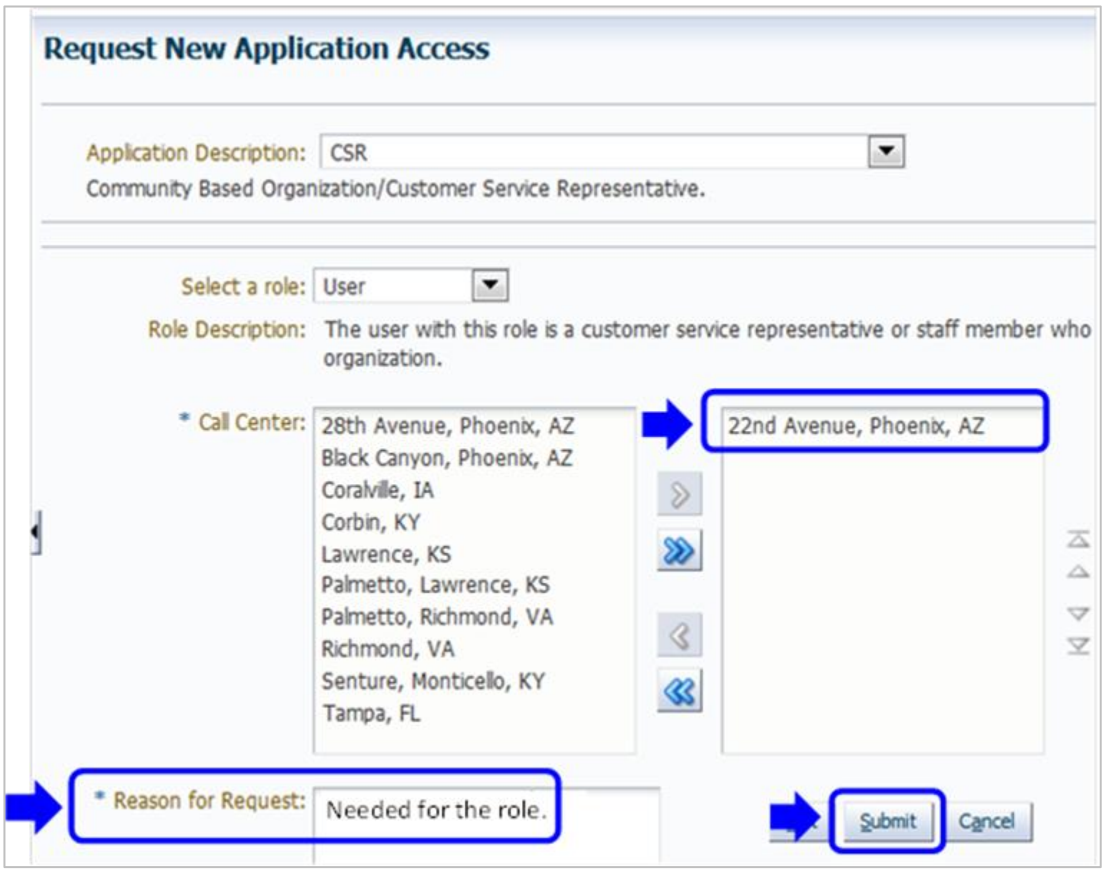
Required fields are marked with an asterisk (*) and an error message displays, if the information has not been entered or selected correctly, or is entered in the wrong format.

Note
If all of your business contact information is on file, the **"Please update your profile…"** message does not display and the **Select a role** drop-down list displays for you to continue.

If the **"Please update your profile…"** message displays, enter the required information and then select **Next**.



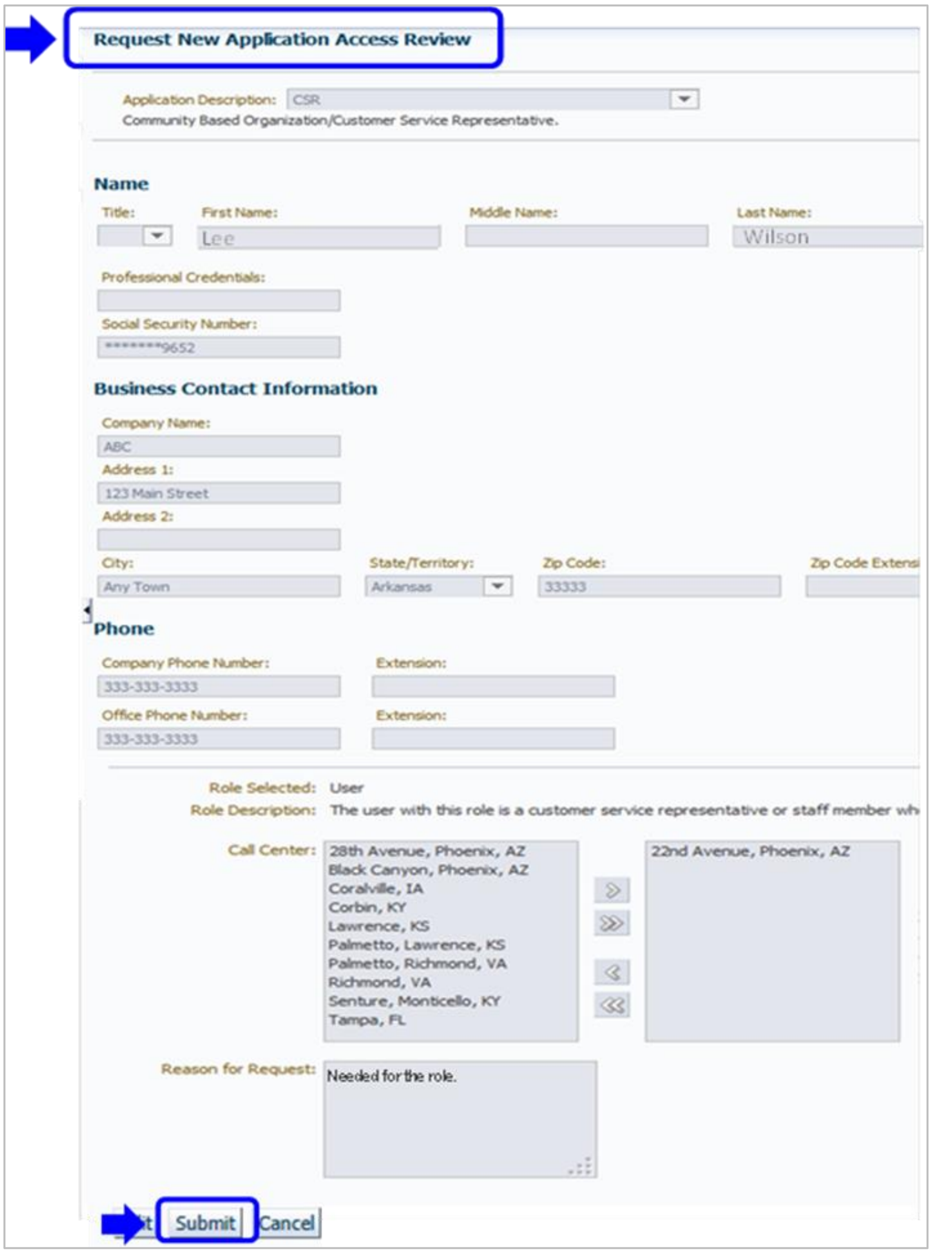
Action	
Step 6	After providing your business contact information, EIDM may ask you to provide some additional information that is required for your application and the role you have selected. Provide any additional information that is requested, enter a reason for the request in the **Reason for Request** box and then select **Submit**. **Note** What You May Need Before You Begin In the example below, we selected the CSR application and the **User** role. EIDM also needs to know the Call Center. We selected 22nd Avenue, Phoenix, AZ from the list of Call Centers and then selected the single right arrow icon. This moved the 22nd Avenue, Phoenix, AZ Call Center to the Selected Call Center(s) box. We then entered the reason for the request in the **Reason for Request** box and select **Submit** to continue the process.



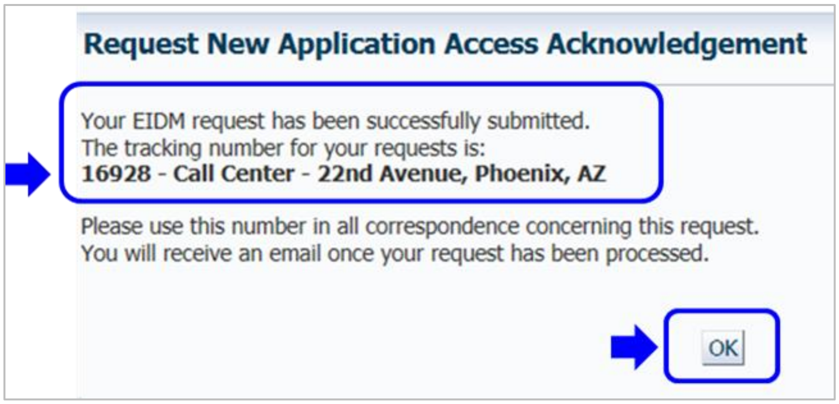
	Action
Step 7	After selecting Submit, the **Request New Application Access Review** page displays. Review the information displayed. Select **Edit** to modify the information. Select **Submit** to submit the request for approval.

Note

You may select **Cancel** to exit out of the Request New Application Access process. New information or changes entered do not save.



Step 8	Action
	After selecting Submit, the **Request New Application Access Acknowledgement** page displays. The acknowledgement page displays the tracking number for the request and informs you that you should receive an e-mail when the request has been processed. **Note** If you have submitted a request for a role in an application where a CMS 4-character Resource Access Control Facility (RACF) is used for identification and verification, you may have to change your password and create and enter an 8-character password the next time you log in, after your request has been approved. An 8-character password may be required for applications that use RACF IDs. Select **OK** to close the acknowledgment page.



To request a role for one of the applications listed below:

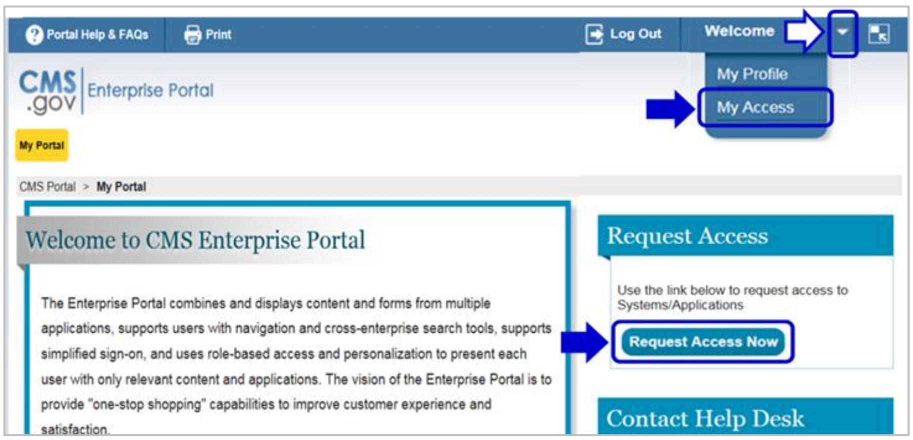
- ASETT
- ASP
- EPPE
- ESD
- FFM/Training–Agents/Brokers/Assisters
- IC
- IDHD
- MACPro
- MCU
- MLMS
- Open Payments
- SHIM
- T-MSIS
- zONE

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.



Step 2	The application **Access Catalog** displays.

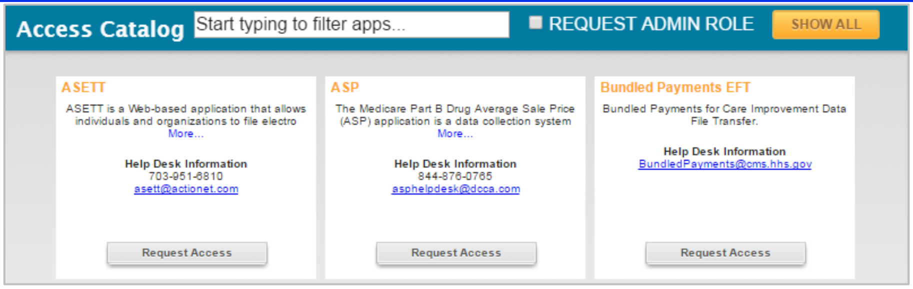
Scroll down to locate the application you need.

Alternatively, enter the first few letters of the application in the **Search** section and all of the applications beginning with those letters display.

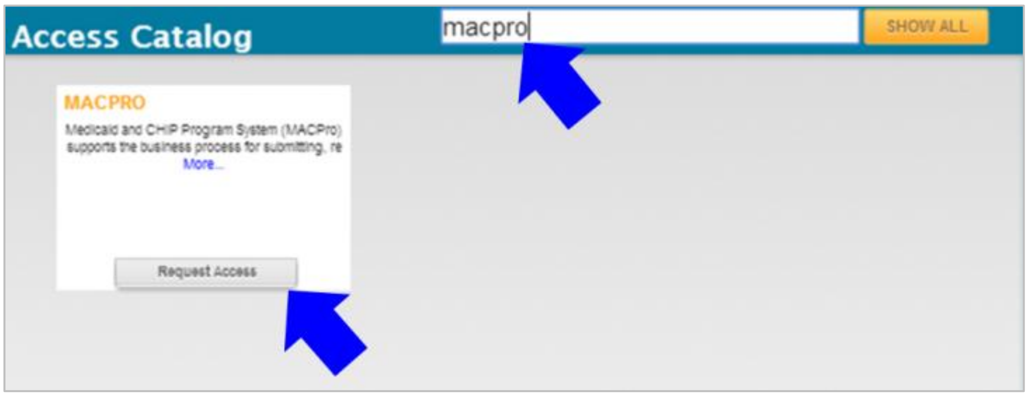
Notes

- The applications are listed by their acronym not their full name. You must use the acronym of the application to search.
- If you currently have access to one or more applications, those applications are displayed in the **My Access** section. If you have pending requests, they are displayed in the **My Pending Requests** section.

Action



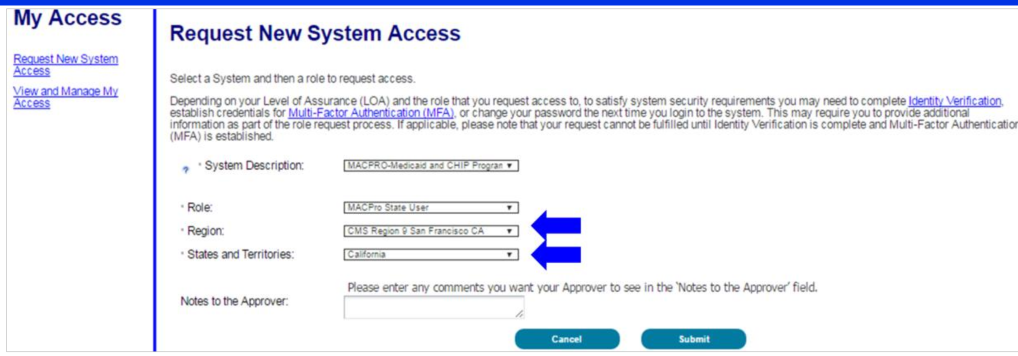
Step 3 Select the **Request Access** button on the application tile.



Step 4 The **Request New System Access** page for that application displays.

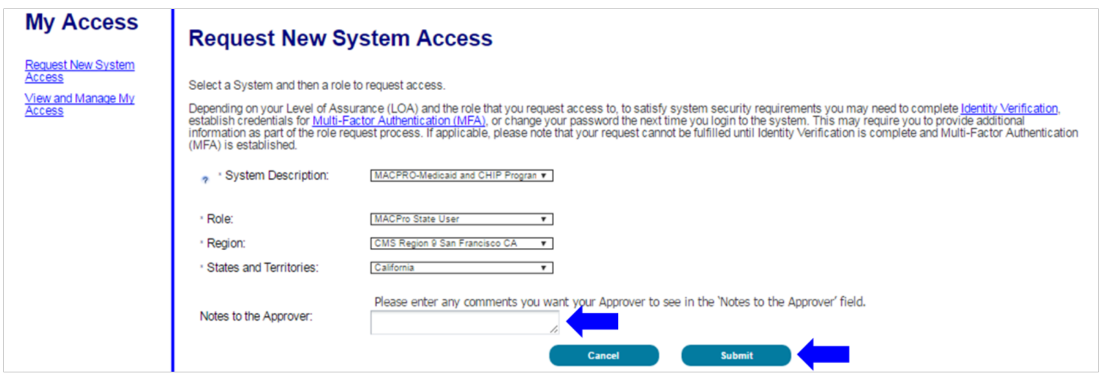
Select a **Role** from the drop-down list. There may also be additional information that you need to provide to request a role, such as **State**, **Region**, **Authorization Code**, **User Type**, or other user information.

Action



Step 5 Select the **Submit** button to submit the request. To terminate the request, select the **Cancel** button and the system returns you to the **View and Manage My Access** page.

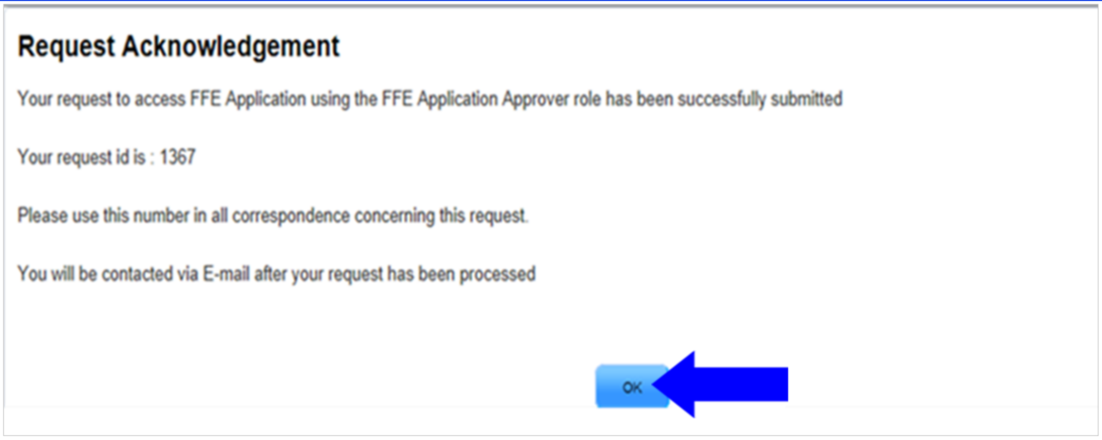
Depending on the application selected, you may have the option of entering a message in the **Notes to the Approver** field shown below.



Step 6 After submitting the request, a Request Acknowledgement message displays. Select the **OK** button to exit the screen and return to the **View and Manage My Access** page.

Note
If you have selected an application that does NOT have 'automatic' online approval, the request is evaluated by the application approver. You should receive an e-mail once the approver takes an action on the role request.

Action

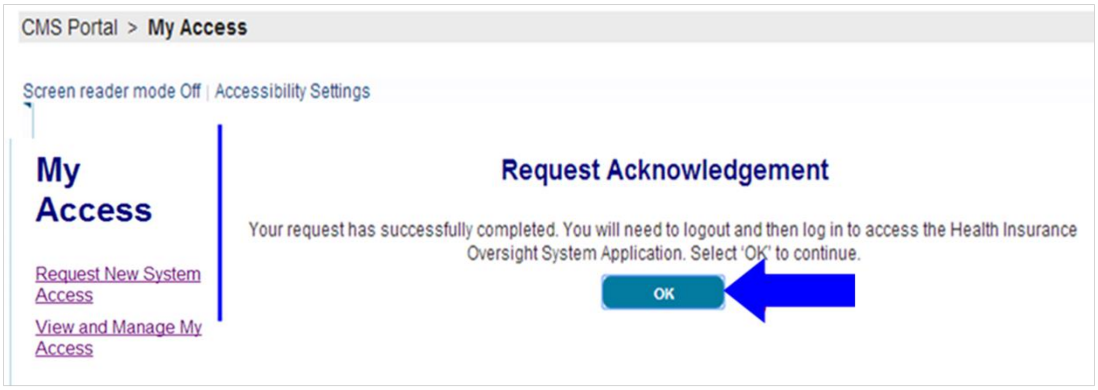

Request Acknowledgement
Your request to access FFE Application using the FFE Application Approver role has been successfully submitted
Your request id is : 1367
Please use this number in all correspondence concerning this request.
You will be contacted via E-mail after your request has been processed
OK

Step 7	Action
	If you have selected an application that has 'automatic' online approval and you have entered valid information, you should receive a message similar to the one below for the application that you have chosen.

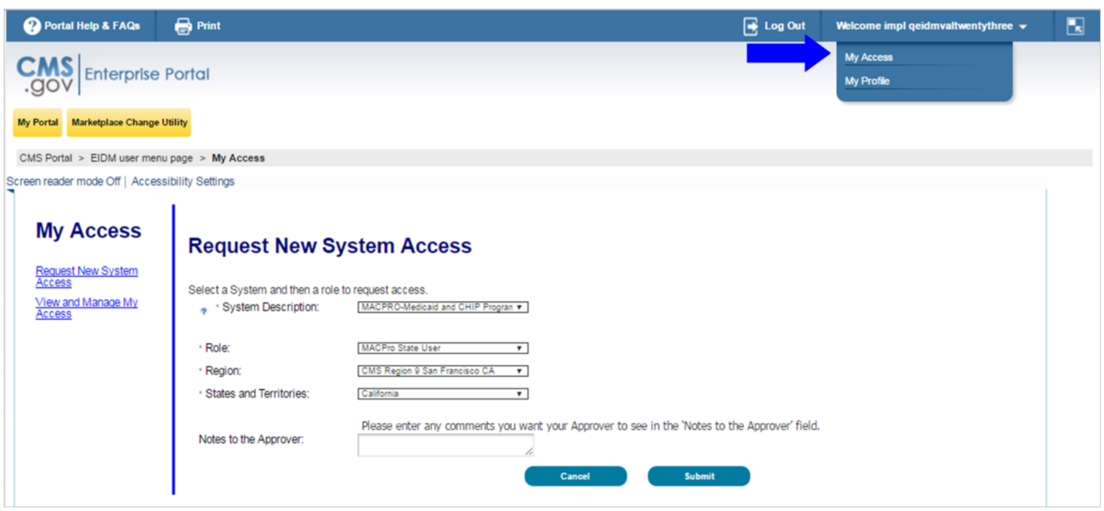
Select the **OK** button to exit the screen and return to the **View and Manage My Access** page.

Note

To access the requested application, you need to logout and log back in.



You may return to the **Access Catalog** at any time by selecting the **My Access** option from the drop-down list.



How to Cancel a Pending Role Request

The following are the basic step-by-step instructions on how to cancel a pending role request.

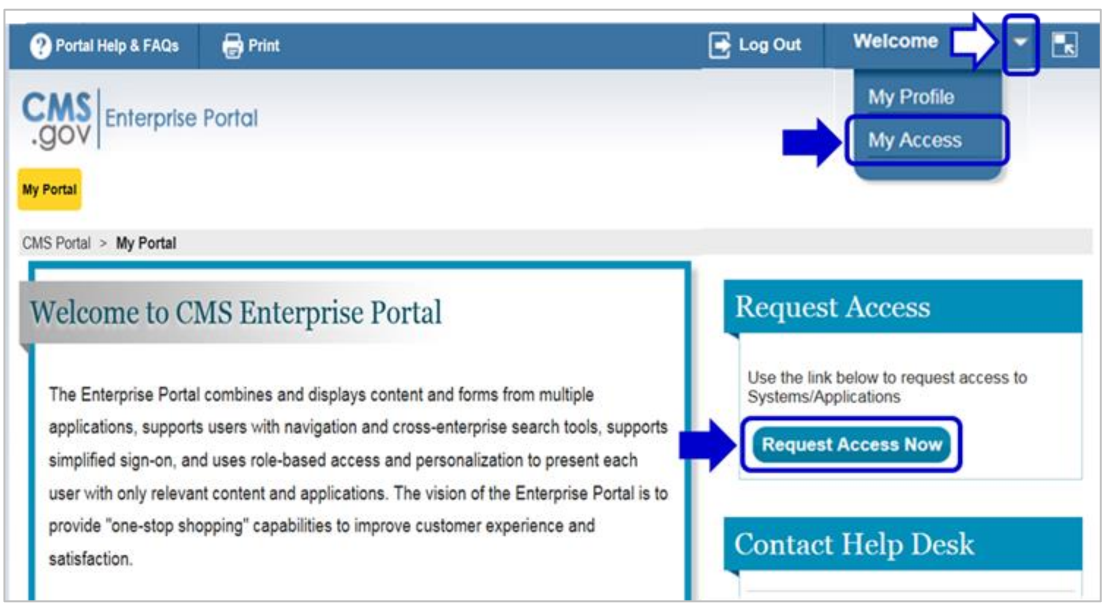
Important Note

To cancel a role for one of the applications listed below:

- ASETT
- ASP
- EPPE
- ESD
- FFM/Training– Agents/Brokers/Assisters
- IC
- IDHD
- MACPro
- MCU
- MLMS
- Open Payments
- SHIM
- T-MSIS
- zONE

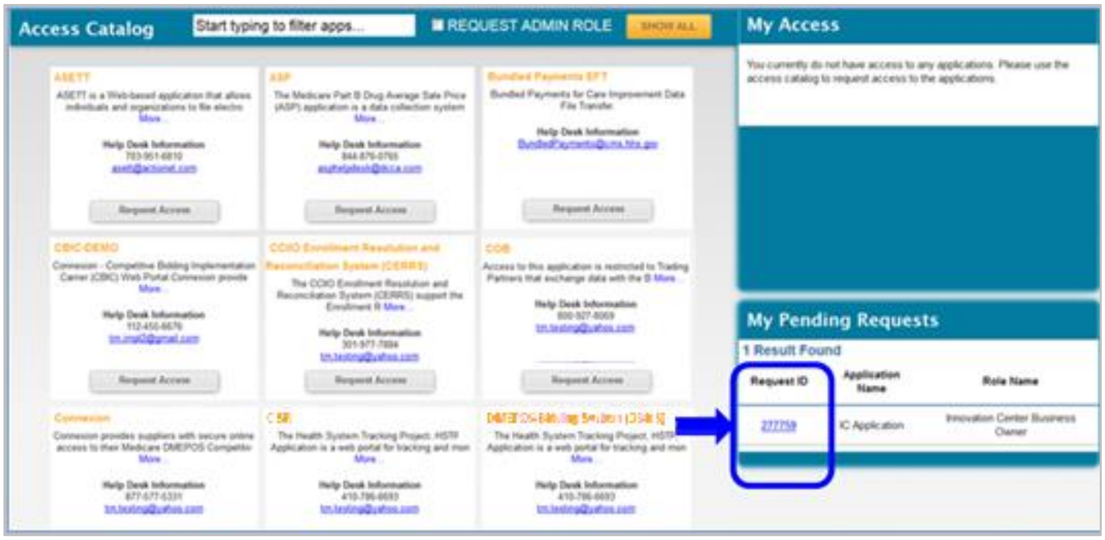
To cancel a pending role request for all other applications, please **FOLLOW THESE STEPS**.

	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.



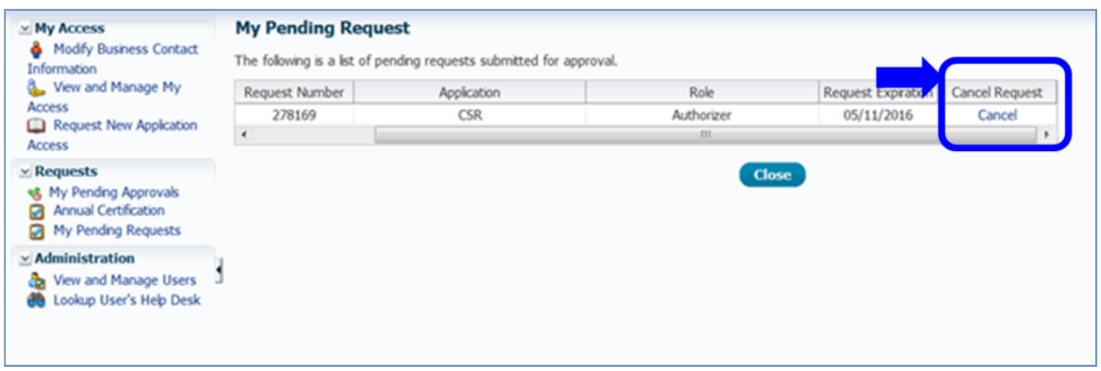
	Action
Step 2	The application **Access Catalog** displays.

In the **My Pending Requests** section of the Access catalog, select the **Request ID** link for the pending request.



Step 3	The **Pending Requests** panel displays on the **View and Manage My Access** page.

In the **Cancel Request** column, select the **Cancel** link for the role request you wish to cancel.

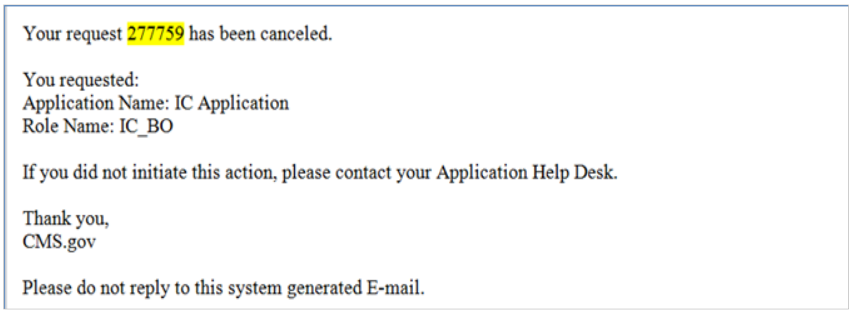


Step 4	A pop-up confirmation displays. Select **OK** to submit the request.

Action

Step 5 The pending role request is removed from the **Pending Requests** queue and a confirmation message displays.

Step 6 You should receive an e-mail notification that the role request has been cancelled.



Your request 277759 has been canceled.

You requested:
Application Name: IC Application
Role Name: IC_BO

If you did not initiate this action, please contact your Application Help Desk.

Thank you,
CMS.gov

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

> **Note**
>
> An e-mail notification of the role request cancellation is sent to both the user and the approver of the application.

To cancel a role for one of the applications listed below:

- ASETT
- ASP
- EPPE
- ESD
- FFM/Training–Agents/Brokers/Assisters
- IC
- IDHD
- MACPro
- MCU
- MLMS
- Open Payments
- SHIM
- T-MSIS
- zONE

Please **FOLLOW THESE STEPS**:

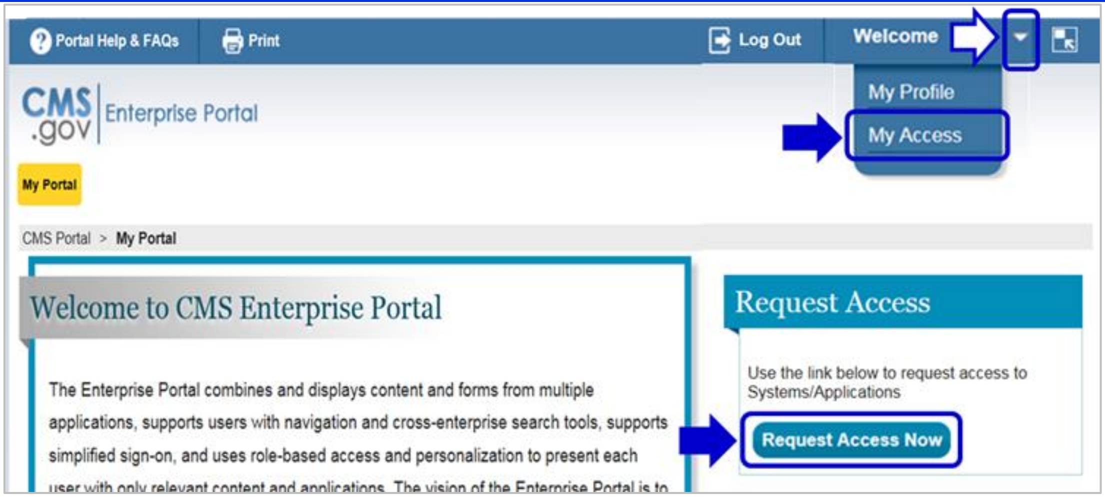
Action

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.

Action

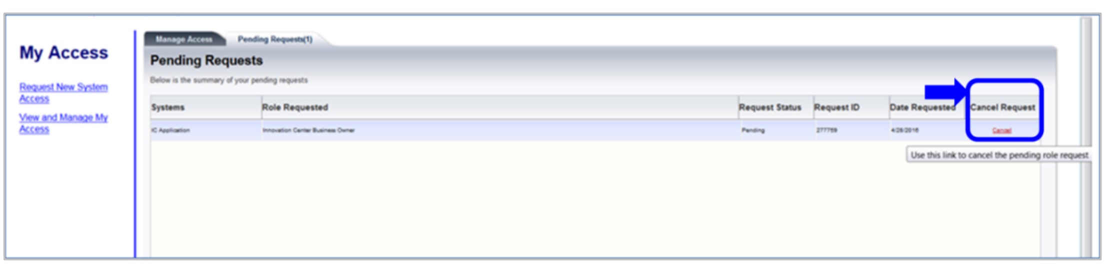


Step 2 The application **Access Catalog** displays.

In the **My Pending Requests** section of the Access catalog, select the **Request ID** link for the pending request.

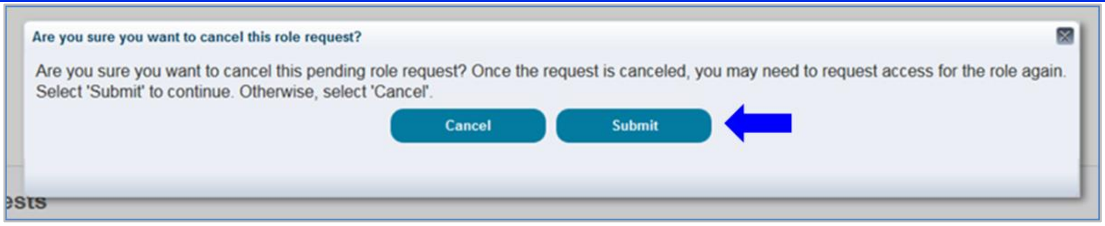
Step 3 The **Pending Requests** panel displays on the **My Access** page.

In the **Cancel Request** column, select the **Cancel** link for the role request you wish to cancel.

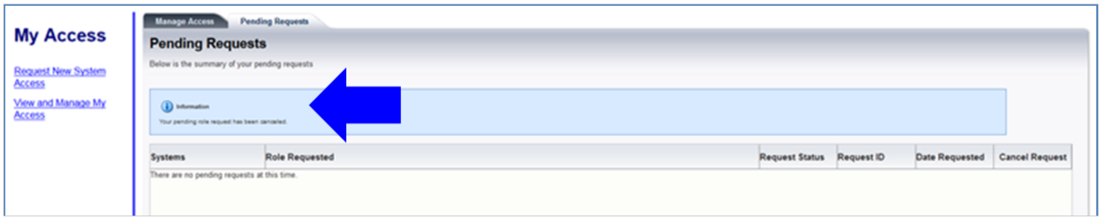


Step 4 A pop-up confirmation displays. Select **Submit** to submit the request.

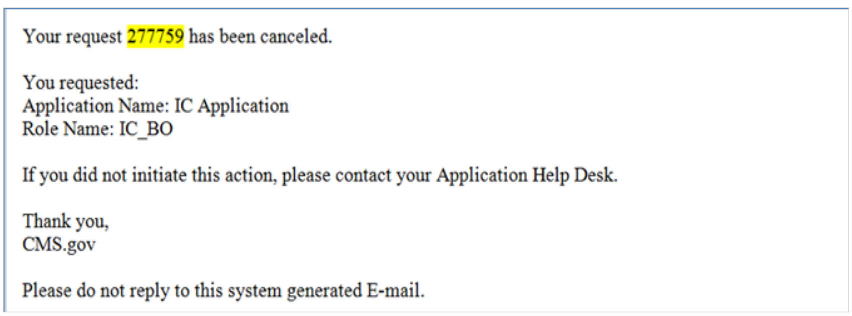
Action



Step 5 The pending role request is removed from the **Pending Requests** queue and a confirmation message displays.



Step 6 You should receive an e-mail notification that the role request has been cancelled.


Your request 277759 has been canceled.

You requested:
Application Name: IC Application
Role Name: IC_BO

If you did not initiate this action, please contact your Application Help Desk.

Thank you,
CMS.gov

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

Note

An e-mail notification of the role request cancellation is sent to both the user and the approver of the application.

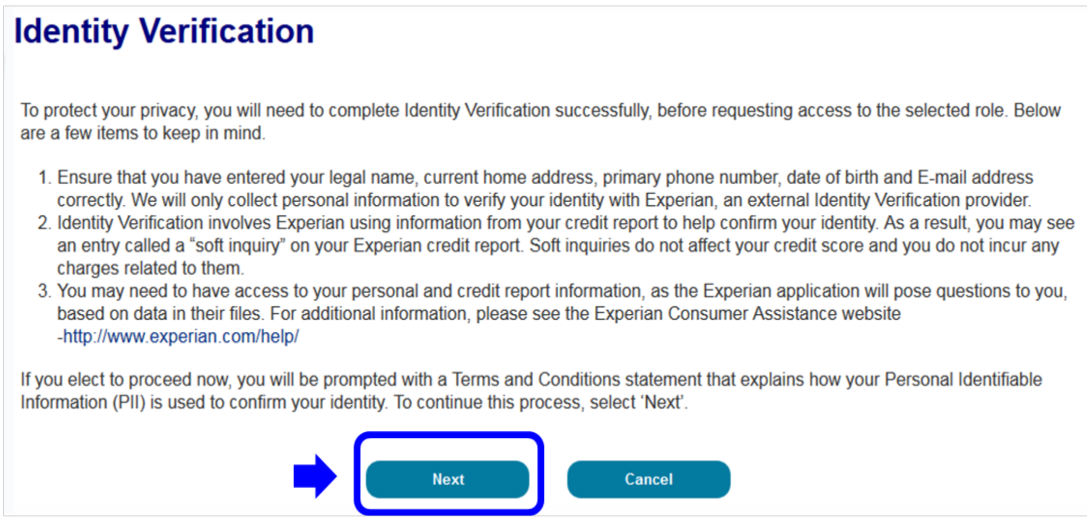
Identity Verification

Depending on the role and the information you provide, the system may take you to the Identity Verification page. The Identity Verification process, also known as Remote Identity Proofing (RIDP), is necessary for roles that require a higher level of security to access. Identity Verification is done by asking you questions based on your personal information.

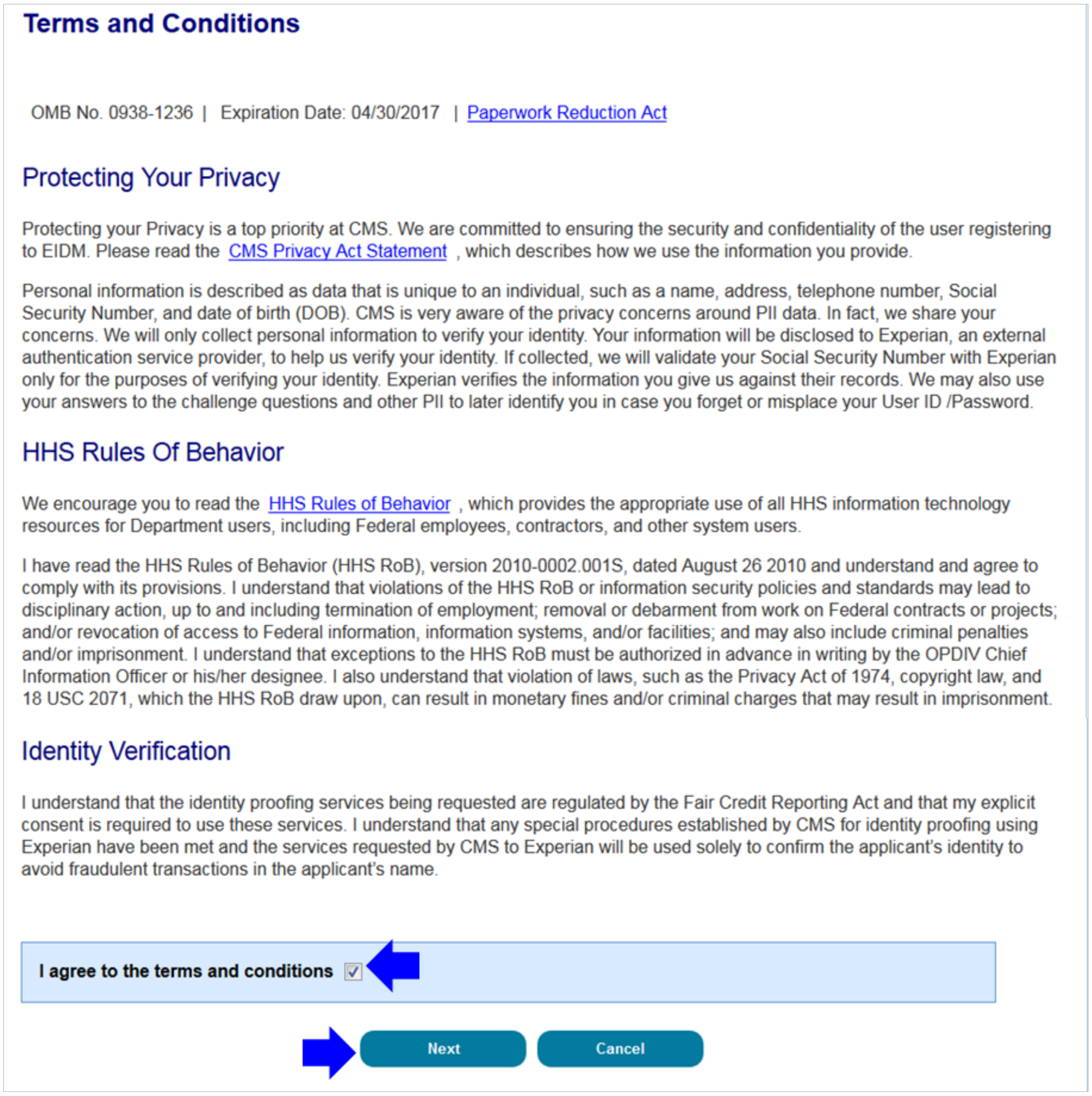
Note
CMS uses credit reporting agencies like Experian to verify identity information. This is only an inquiry and does not affect your credit score.

To begin the Identity Verification process, **FOLLOW THESE STEPS**:

	Action
Step 1	If you select a role that requires identity verification, the **Identity Verification** page displays. Select **Next** to begin the Identity Verification process.



	Action
Step 2	Read the important **Terms and Conditions** information on this screen and indicate your agreement by selecting the **I agree to the terms and conditions** checkbox. Select the **Next** button to continue.



Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 | Paperwork Reduction Act

Protecting Your Privacy

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement , which describes how we use the information you provide.

Personal information is described as data that is unique to an individual, such as a name, address, telephone number, Social Security Number, and date of birth (DOB). CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal information to verify your identity. Your information will be disclosed to Experian, an external authentication service provider, to help us verify your identity. If collected, we will validate your Social Security Number with Experian only for the purposes of verifying your identity. Experian verifies the information you give us against their records. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

HHS Rules Of Behavior

We encourage you to read the HHS Rules of Behavior , which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

I have read the HHS Rules of Behavior (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

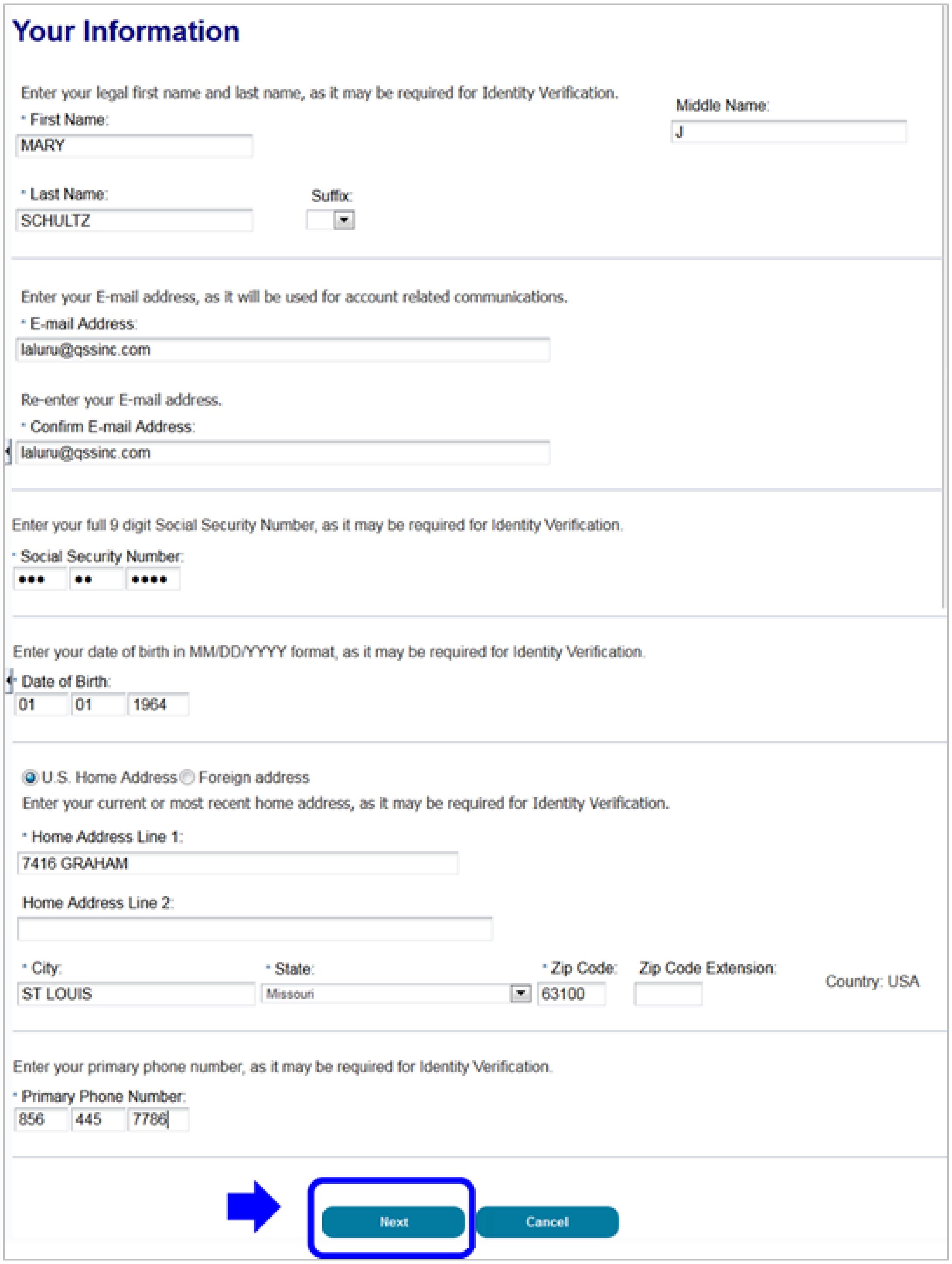
Identity Verification

I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

I agree to the terms and conditions ☑

Next Cancel

	Action
Step 3	Enter your information into the required fields of the **Your Information** page. Select **Next** to continue the Identity Verification process.

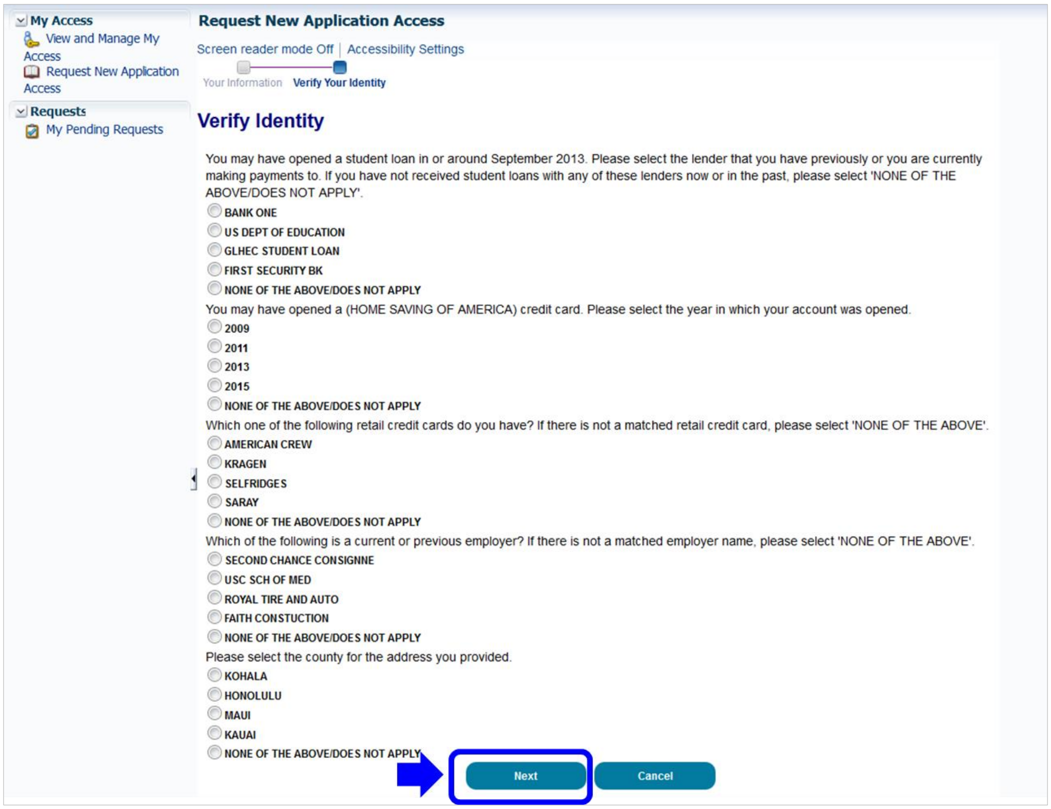


Action

Step 4

Depending on the information you provided, the **Verify Identity** page may be displayed. You are required to answer several questions about information that may be in your personal records. Please answer the questions to the best of your ability.

Select the **Next** button to submit the request. If you wish to terminate the request, select **Cancel** to return to the **View and Manage My Access** page.

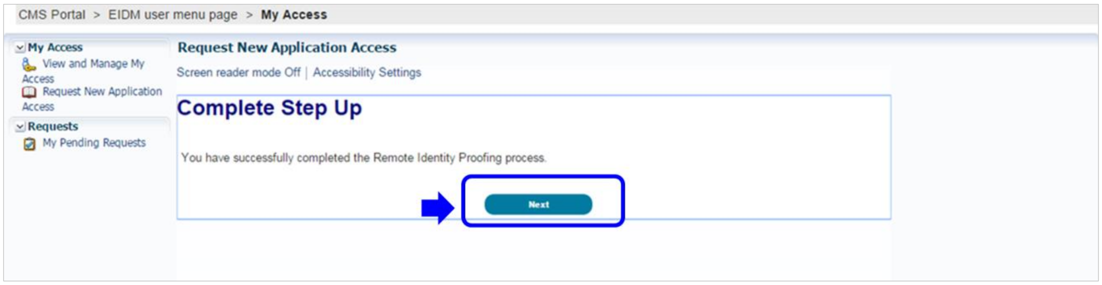


Step 5

After submitting the request, the Identity Verification confirmation displays. Select the **Next** button to continue with the role request process.

Note

If the role auto-approves, the role is granted; log out and log back in to access it.



Identity Cannot be Verified

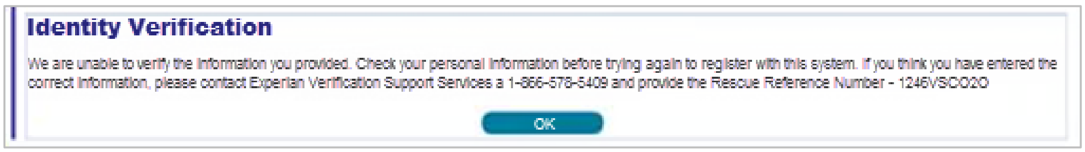
If you receive an error message that your identity cannot not be verified, it may simply mean that the information you provided could not be matched with the information available in the electronic records used for verification. You may need to take some additional steps to verify your identity.

Please follow the steps below.

Action

Step 1 Check your personal information before trying again to register with the system.

Step 2 If you have entered the correct information and still cannot be verified, you are instructed to call the Experian Help Desk and provide the **Review Reference Number** displayed on the screen so the help desk representative can help you verify your identity. Experian is the contractor CMS uses to complete the Identity Verification process.



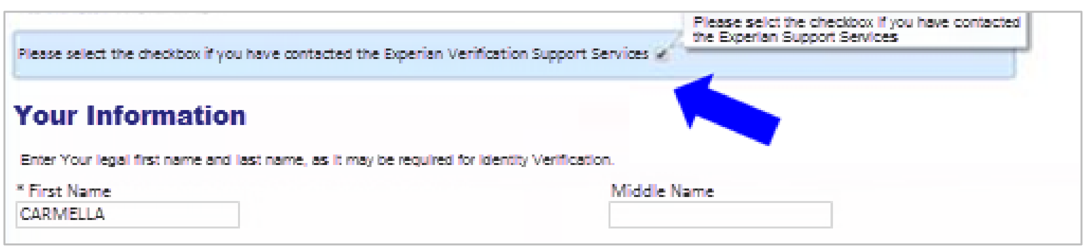
Step 3 After you have contacted Experian login to CMS Enterprise Portal and proceed again through Role Request process *(see How to Request a Role*

for the steps).

Step 4 On the **Your Information** screen, select the check box if you have contacted Experian and completed the identity verification process over the phone with the Experian Support personnel.

> **Note**
>
> Selecting this checkbox instructs the system to retrieve your identity verification results from Experian based on the phone verification process. You do have the option of not selecting the checkbox and continuing as you did in your original attempt of Identity Verification, prior to contacting Experian.

Enter your information in the required fields.



Step 5 If your identity cannot not be verified by Experian, please contact your Application Help Desk for the next steps *(see Appendix B: Application Help Desk Information for the contact information)*.

Action
Note Depending on the type of role you requested, you may not be granted the role you requested until you have successfully undergone ID proofing.

Multi-Factor Authentication (MFA) Registration

Multi-Factor Authentication (MFA) is a security mechanism that is implemented to provide an extra layer of security such as a security code, when logging in with your User ID and Password..

Registered CMS portal users who wish to access a CMS MFA protected application are directed through the MFA registration process.

During the MFA registration process, the CMS EIDM system requires registration of a phone or computer to add an additional level of security to a user's account. The user is given five options from which to select, to complete the registration process:

- **Smart Phone**: Users can download VIP access software on their smart phone/tablet. The user must enter the alphanumeric Credential ID that is generated by the VIP access client. The user then enters the Security Code generated by the VIP client.
- **Computer**: Users can download VIP access software on their computer. The user must enter the alphanumeric Credential ID generated by the VIP access client. The user enters the Security Code generated by the VIP client.
- **Short Message Service (SMS)**: Users can use the SMS option to have their Security Code texted to their phone. The user must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR)**: The user can select the IVR option to receive a voice message containing their Security Code. The user must provide a valid phone number and (optional) phone extension.
- **E-mail**: Users can select the e-mail option to receive an e-mail containing the Security Code required at login. The e-mail address on the user's profile is used.

Notes

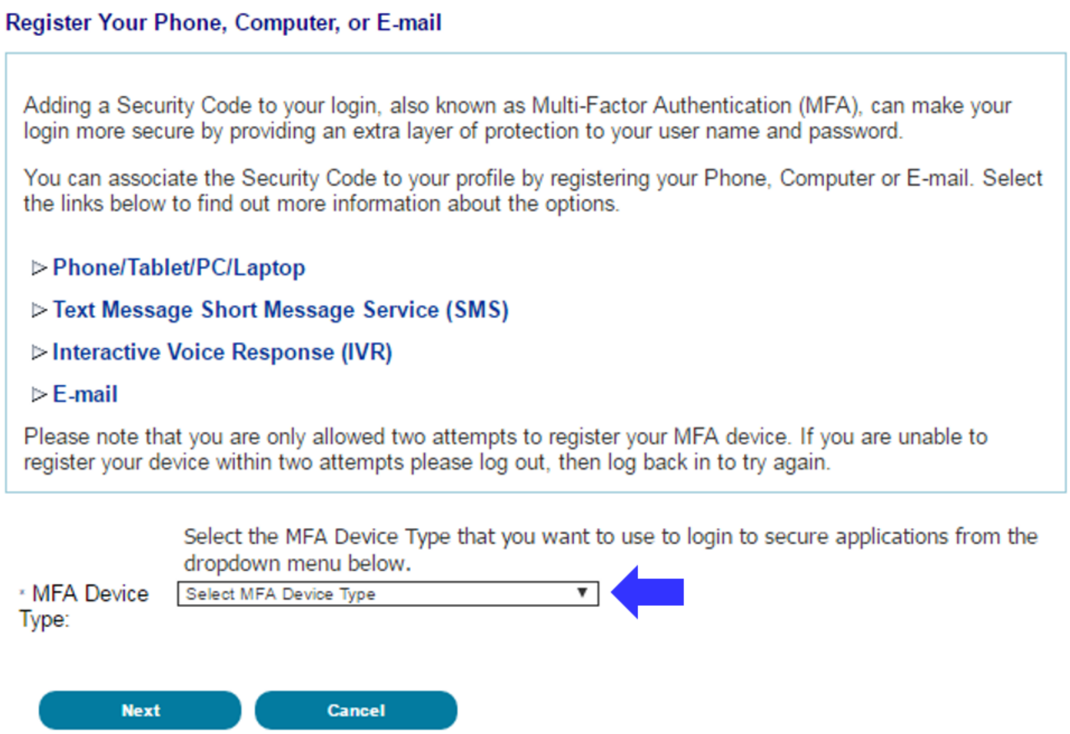
- Delays in e-mail transmission, spam filters, and other issues outside the user's control can make this the least desirable option to receive a security code.
- Users can register more than one phone number for the SMS device type. Symantec will only use one number (the lowest number by area code) to send the Security Code.
- While the 'Security Code' for the VIP Access Software refreshes automatically every 30 seconds, the 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expire in 30 minutes. The 'Security Code' for the other MFA device types expire in 10 minutes. If you are unable to enter the code within the allotted period, you must request a new one.

To gain access to a CMS MFA-protected application, **FOLLOW THESE STEPS**:

Action

Step 1 If you select a CMS MFA-protected application, the **Multi-Factor Authentication Information** page displays. Select **Next** to begin the MFA Registration process.

Step 2 To make your account more secure, you are directed to the **Register Your Phone, Computer, or E-Mail** page. Select the **MFA Device Type** you wish to register from the drop-down list.



Notes

- **For VIP Client**: Enter the Credential ID generated by the VIP Access client.
- **For Text**: You have to enter a valid phone number to receive your Security Code.
- **For Interactive Voice Response (IVR)**: Enter the phone number and (optional) extension to be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks'*'; period '.'; comma ','; pound '#', followed by numeric 0 to 9. For example: 4885554444, 1112.

  , (comma) Creates a short delay of approximately 2 seconds;

  . (period) Creates a longer delay of approximately 5 seconds;

Action

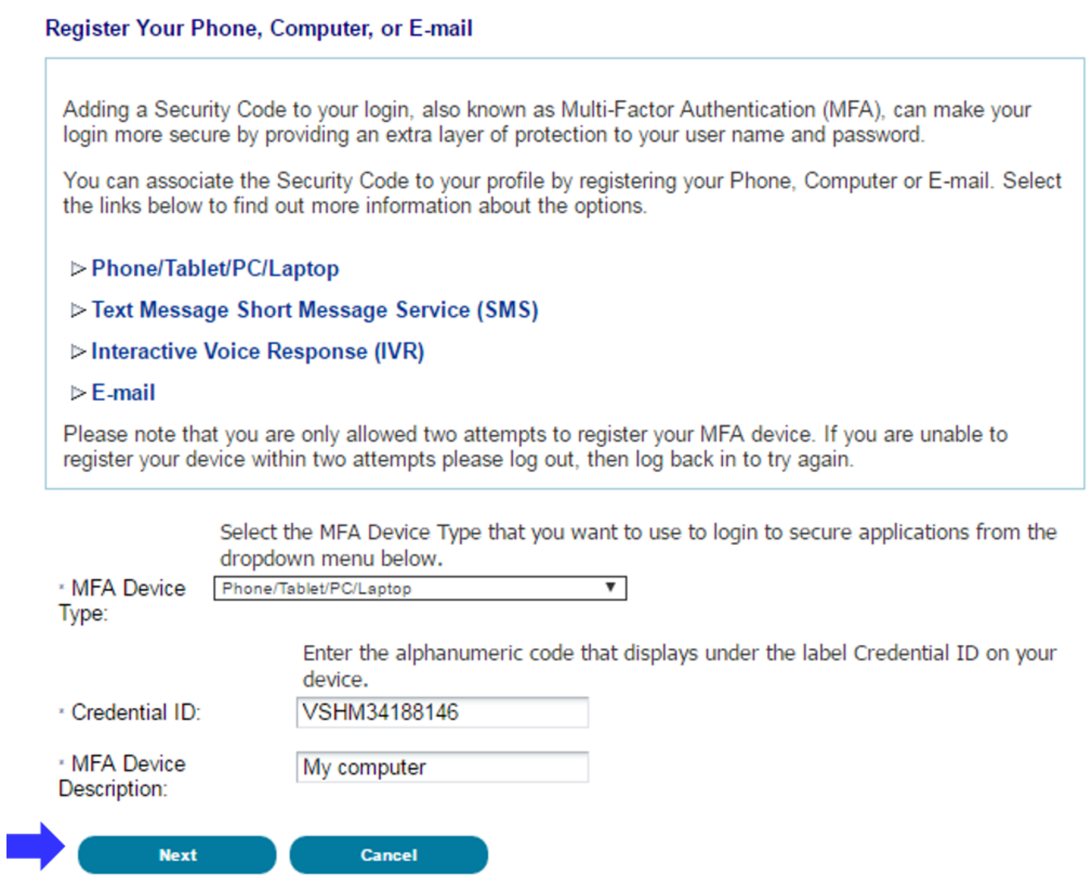
***(asterisks)** Used by some phone systems to access an extension;
 # (pound/hash) Used by some phone systems to access an extension; and

- You may use a comma if you are not sure of the special character supported by your company's phone system.
- **For E-mail**: The e-mail on your profile is used to send the Security Code required at login.

Using the VIP Client

1. Depending on the option you select, download the VIP Access software from the URL provided on the **Register Your Phone or Computer** page.
2. Once downloaded, select the **VIP Access Icon** on your desktop to activate the **VIP Access** window.
3. Select the pages icon next to the **Credential ID** to copy the alphanumeric code.
4. Place your curser in the **Credential ID** on the **Register Phone or Computer** page and right click to paste it in.

Step 3 Enter the credentials of the device (VIP Client shown) and a short description in of the device in the **MFA Device Description** field. Then select **Next** to submit your registration.


Register Your Phone, Computer, or E-mail

Adding a Security Code to your login, also known as Multi-Factor Authentication (MFA), can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Select the links below to find out more information about the options.

▷ Phone/Tablet/PC/Laptop
▷ Text Message Short Message Service (SMS)
▷ Interactive Voice Response (IVR)
▷ E-mail

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

· MFA Device Type: Phone/Tablet/PC/Laptop

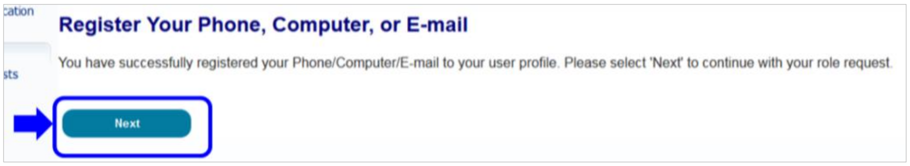
Enter the alphanumeric code that displays under the label Credential ID on your device.

· Credential ID: VSHM34188146

· MFA Device Description: My computer

Next Cancel

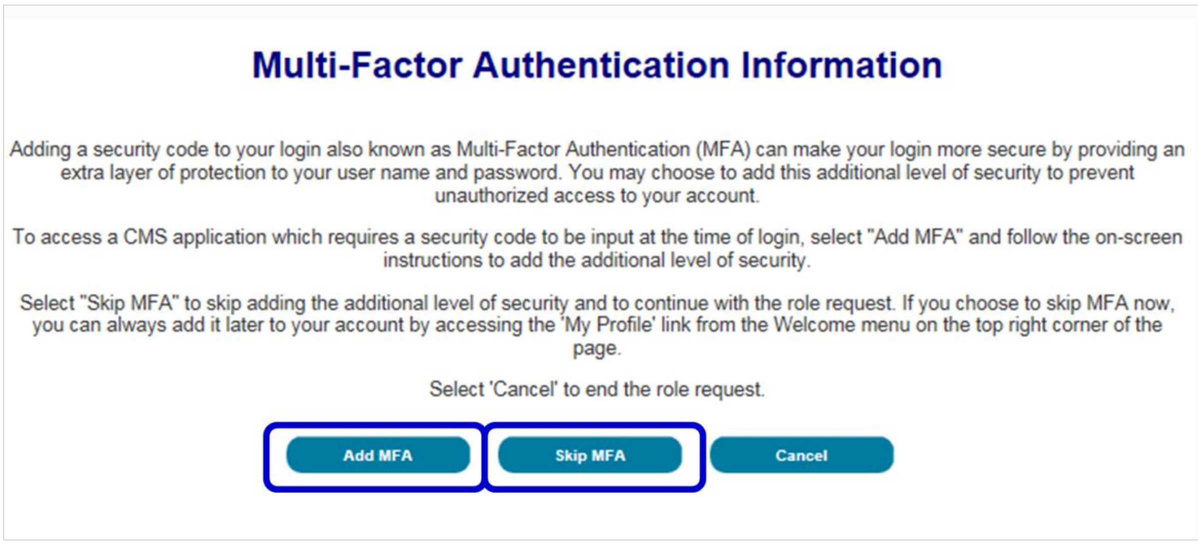
	Action
Step 4	After submitting the registration, a message that you have successfully registered your device displays. Select **Next** to continue the role request process.



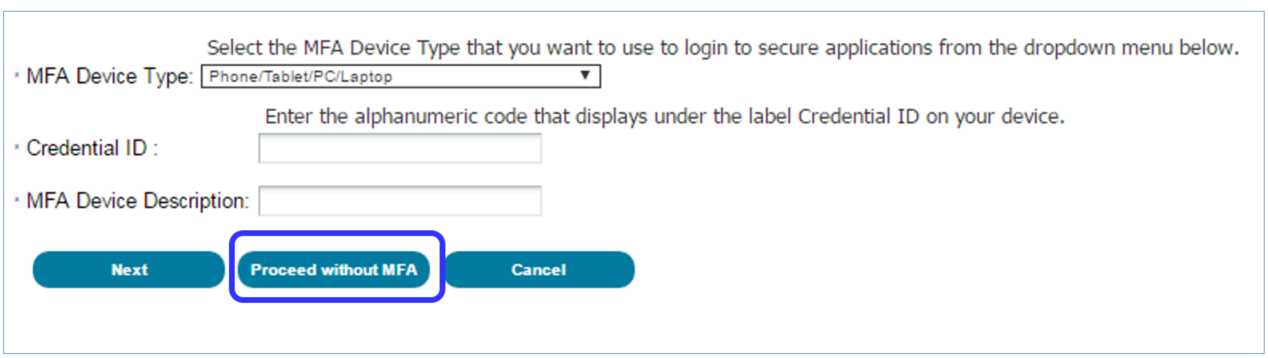
Optional Multi-Factor Authentication (MFA)

Some roles have a reduced level of security requirements and offer MFA as an option to add to their profile.

A user who selects a role that offers MFA as an option is directed to the Multi-Factor Authentication Information Page. The user can select **Add MFA**, to begin the MFA process described in the **Multi-Factor Authentication (MFA) Registration** section, or **Skip MFA**, to skip MFA authentication altogether.



While registering an MFA device, if a user wishes to continue without MFA, he can select **Proceed without MFA**. The user is directed to the next step of the role request process.



6. Checking the Status of a Pending Request

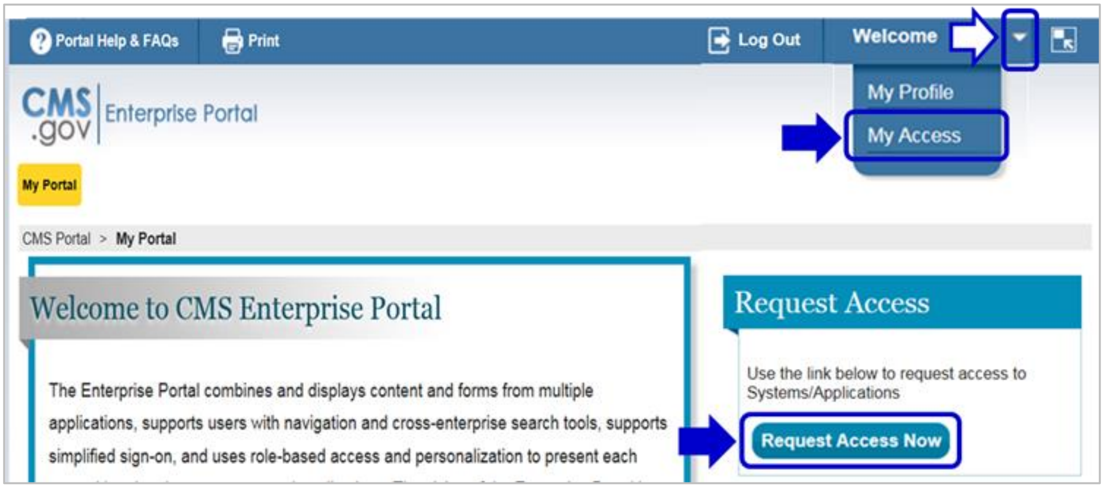
The following are the basic step-by-step instructions on how to use the **My Pending Requests** feature to check the status of a pending request.

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.

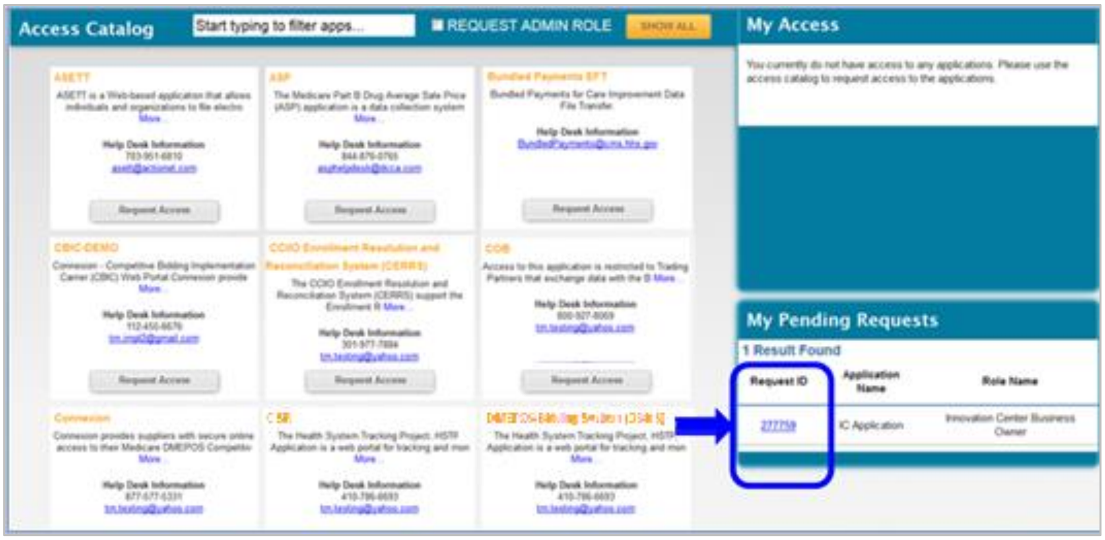
Alternately, you may select **Request Access Now** to continue.



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

Scroll down to **My Pending Requests**. All of your pending requests are displayed in the **My Pending Requests** section.

Select the Request ID number of a pending request to view the details.

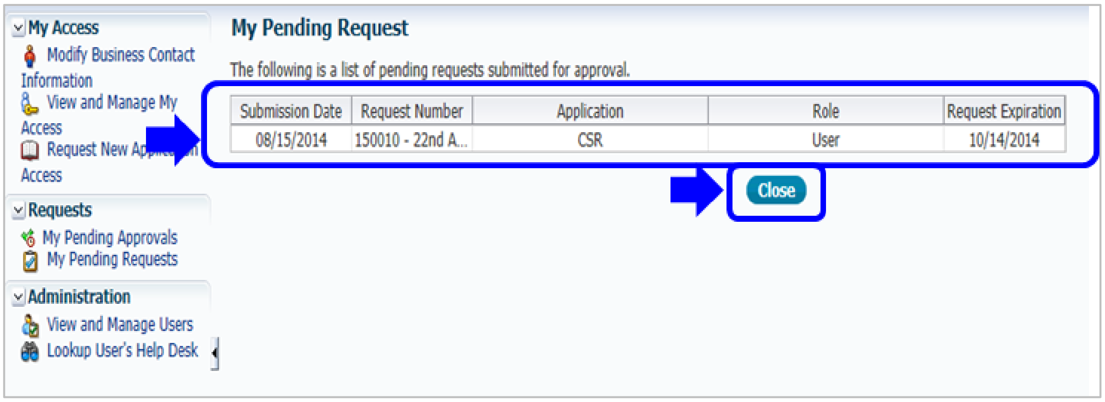


Action	
Step 3	After selecting the Request ID number**,** additional information displays about the pending request.

Note

You should not be able to open or view a pending request. You should receive an e-mail when a pending request has been approved, rejected or has expired.

Select **Close** to close the My Pending Request information.



7. Viewing and Changing Your Access

How to View/Modify Your Business Contact Information

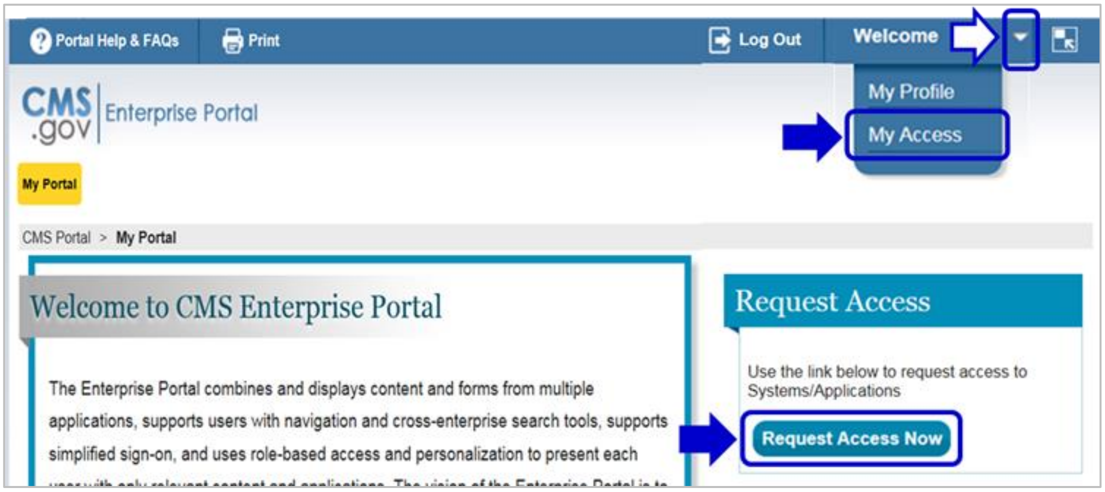
The following are the basic step-by-step instructions on how to use the **Modify Business Contact Information** feature to modify your business contact information.

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.



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

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.

> **Note**
>
> If you currently do not have access to at least one application, the **Available Actions** in the **My Access** section are not displayed. You are not able to modify your business contact information until you have been approved for access to at least one application.

Action

Step 3 After selecting **Other Actions**, the **View and Manage My Access** page displays.

Select Modify Business Contact Information.

Step 4 The **Modify Business Contact Information** page displays. The fields in gray on the **Modify Business Contact Information** page cannot be changed or deleted.

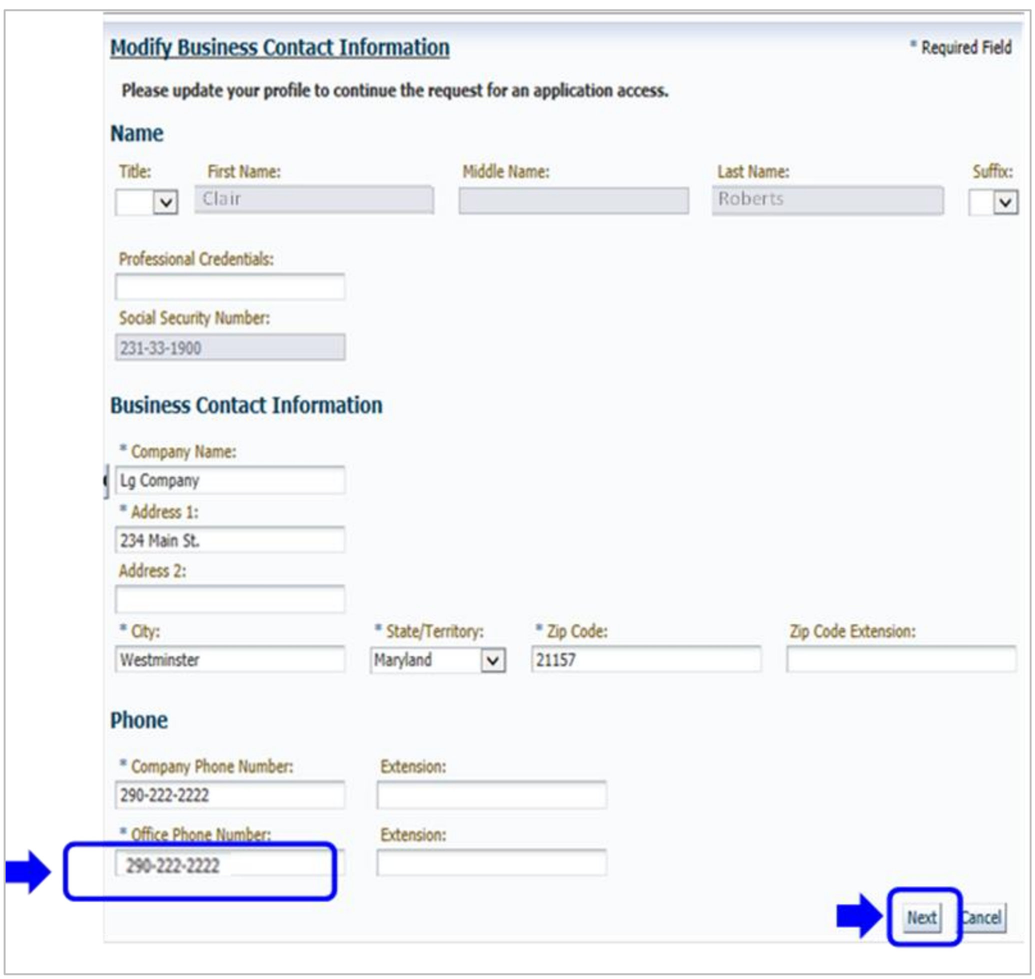
Modify or enter the appropriate information on the **Modify Business Contact Information** page to update your business contact information.

Select **Next** to complete the **Modify Business Contact Information** process.

Note

You may select Cancel at any time to exit out of the Modify Business Contact Information process. New information or changes do not save.

In the example below, we add the Office Phone Number.



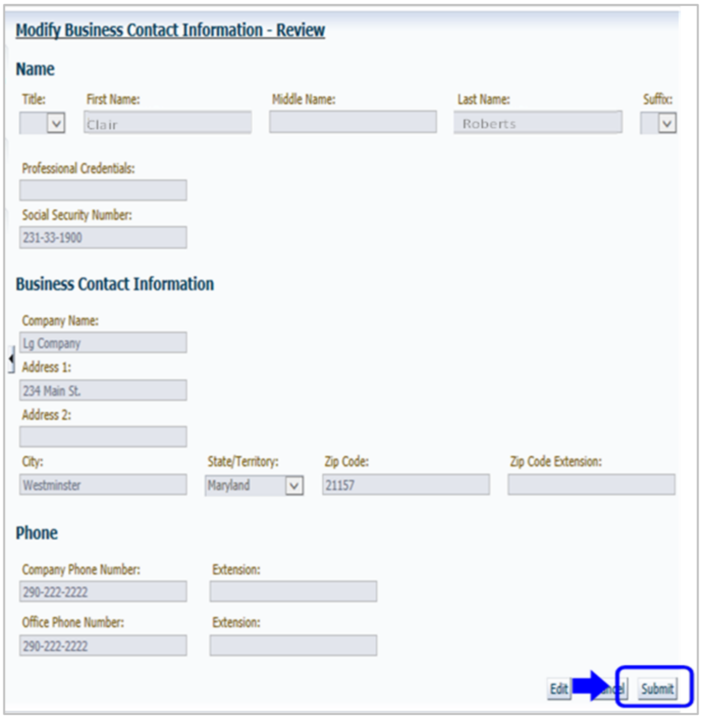
Action

Step 5 The **Modify Business Contact Information - Review** page displays.

Review the information displayed. Select **Edit** to modify the information.

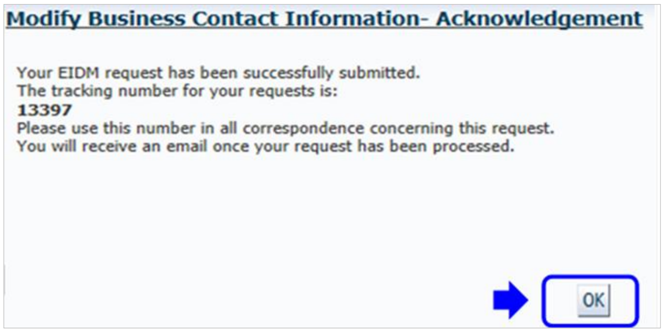
Select **Submit** to submit the request for approval.

> **Note**
>
> You may select **Cancel** to exit out of the Modify Business Contact Information process. New information or changes entered do not save.



Step 6 After selecting Submit, the **Modify Business Contact Information – Acknowledgement** page displays. The acknowledgement page displays the tracking number, for future correspondence, and informs you that you should receive an e-mail when the request has been processed.

Select **OK** to close the acknowledgement page.



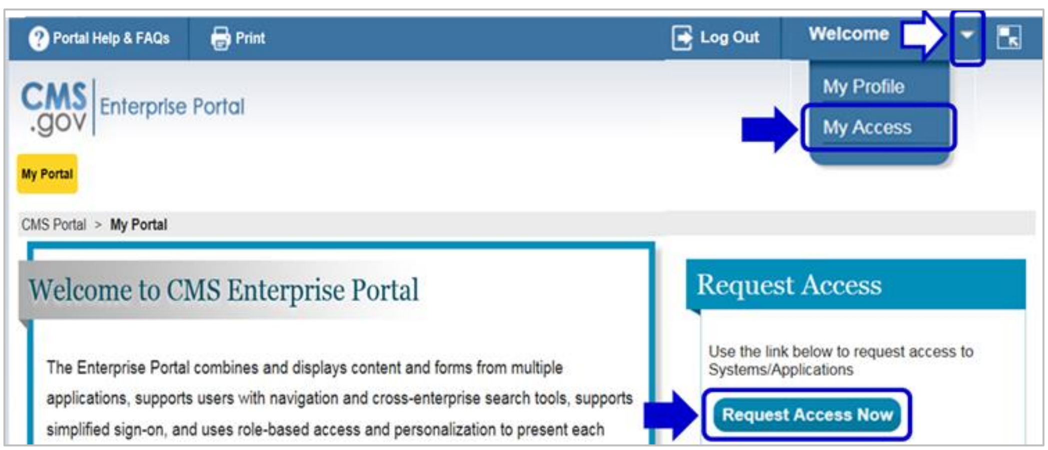
How to View/Modify Your Existing Role Information

The following are the basic step-by-step instructions on how to use the **View/Modify a Role** feature to view/modify your existing role information and add/remove a role attribute, if your application allows you to add/remove an attribute.

- When you registered for a role, you may have also registered for additional features, reports, or other details needed for your role. These are called role “attributes”.
- To view your role information, follow steps 1-5.
- To add an attribute to your role, continue with steps 6-8.
- To remove an attribute from your role, continue with steps 9-13.

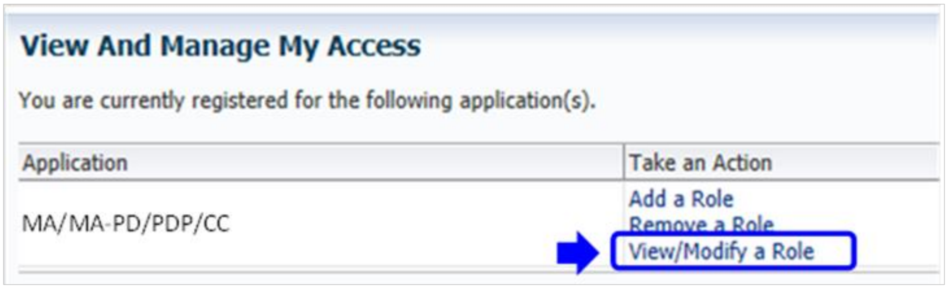
Viewing Your Role Information

To view your role information, follow Steps 1-5.

	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. 
Step 2	The **Access Catalog**, **My Access**, and **My Pending Requests** sections are displayed. Any existing roles you have 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. 

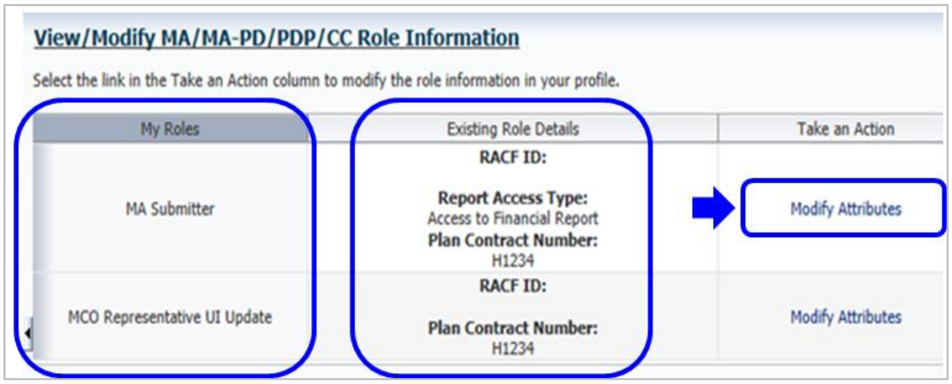
Step	Action
Step 3	The **View and Manage My Access** page displays.

Select **View/Modify a Role** to continue. If there are multiple applications displayed, select **View/Modify a Role** for the application you want to view.



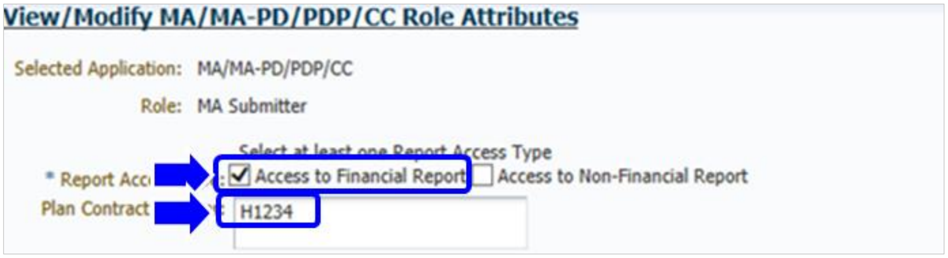
Step 4 The **View/Modify Role Information** page displays.

All of your roles are displayed in the **My Roles** section. All of your existing role information displays in the **Existing Role Details** section. Select **Modify Attributes** to continue. If there are multiple roles displayed, select **Modify Attributes** for the role you want to add a role attribute to.



Step 5 After selecting **Modify Attributes**, the **View/Modify Role Attributes** page displays.

All of your existing role details are also displayed.



Roles without attributes can select **Cancel** to close the page.

Adding an "Attribute" to Your Role

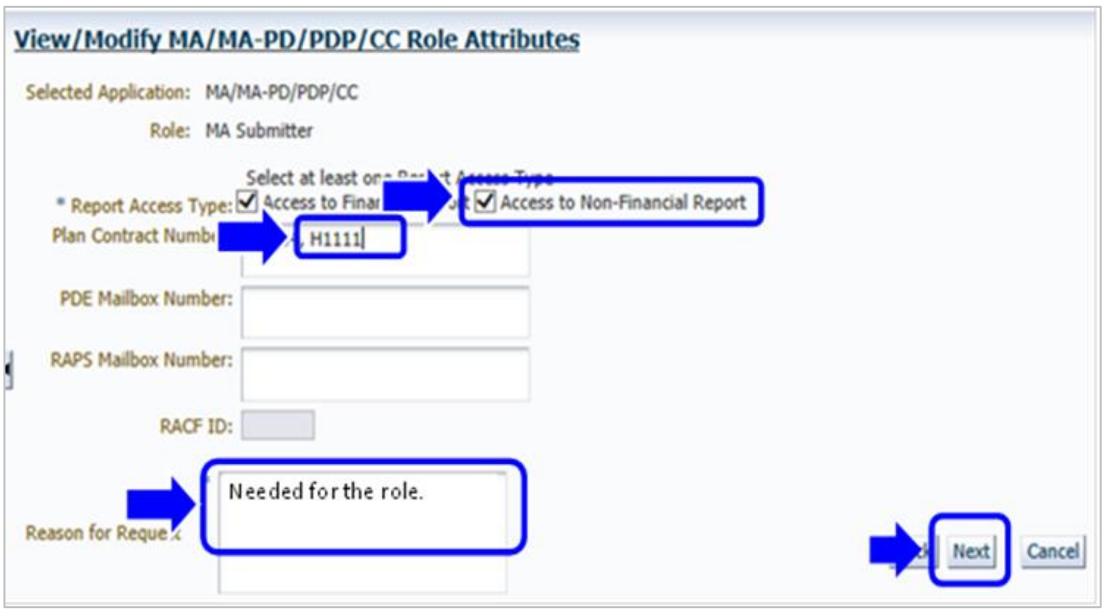
To add an attribute to your role, continue with Steps 6-8.

	Action
Step 6	Provide the additional attributes needed for your role and enter the reason for the request in the **Reason for Request** box.

Select **Next** to complete the **Add a Role Attribute** process.

Note
You may select **Cancel** at any time to exit out of the Add a Role Attribute process. New information or changes entered do not save.

In the example below, we add the **Access to Non-Financial Report** and **Plan Contract Number** H1111, enter the reason for the request in the **Reason for Request** box, and select **Next** to continue.



Step 7 After selecting **Next**, the **View/Modify Role Attributes - Review** page displays.

Review the information displayed. Select **Edit** to modify the information.

Select **Submit** to submit the request for approval.

Note
You may select **Cancel** to exit out of the Add a Role Attribute process. New information or changes entered do not save.

Action

Step 8 After selecting Submit, the **View/Modify Role Attributes - Acknowledgement** page displays.

The acknowledgement page displays the tracking number for the request, the role, and the role attributes to be added.

Select **OK** to close the acknowledgment page.

Removing an "Attribute" from Your Role

To remove an attribute from your role, continue with Steps 9-13.

	Action
Step 9	The **View/Modify Role Information** page displays.

All of your roles are displayed in the **My Roles** section. All of your existing role details are displayed in the **Existing Role Details** section.

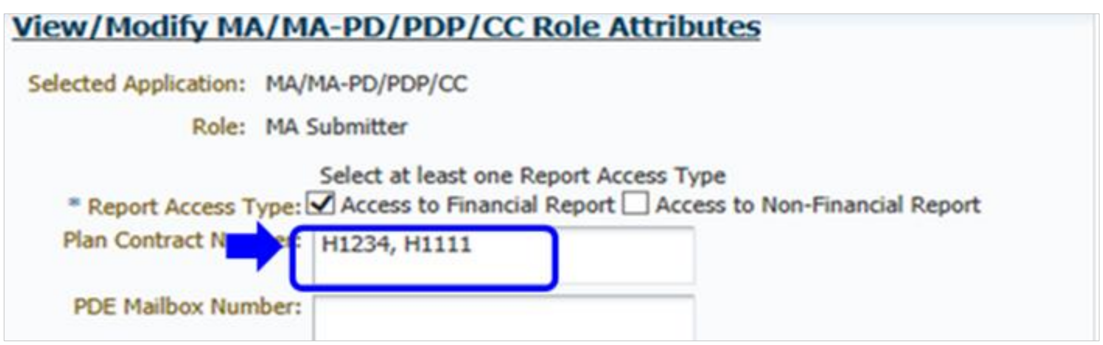
Select **Modify Attributes** to continue. If there are multiple roles displayed, select **Modify Attributes** for the role you want to modify and remove a role attribute.

Note
You may select **Cancel** at any time to exit out of the Remove a Role Attribute process. New information or changes entered do not save.

Step 10	After selecting **Modify Attributes**, the **View/Modify Role Attributes** page displays.

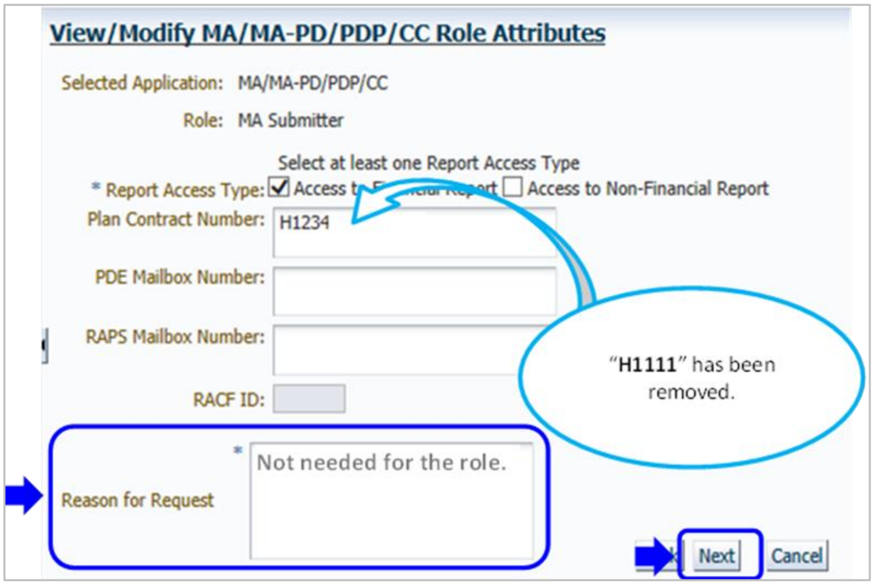
All of your existing role details are also displayed.

Note
Because this screen shows the existing role details, it is imperative that users not remove any of the existing details if access is still needed. Any information deleted from this screen results in a loss of access to the deleted attribute. For this reason, users who wish to add new access should add the additional information while keeping the original details intact.



	Action
Step 11	Remove the attribute or attributes you are required to remove, enter the reason for the request in the **Reason for Request** box, and then select **Next** to continue.

In the example below, we removed **Plan Contract Number** H1111, entered the reason for the request in the **Reason for Request** box, and selected **Next** to continue.

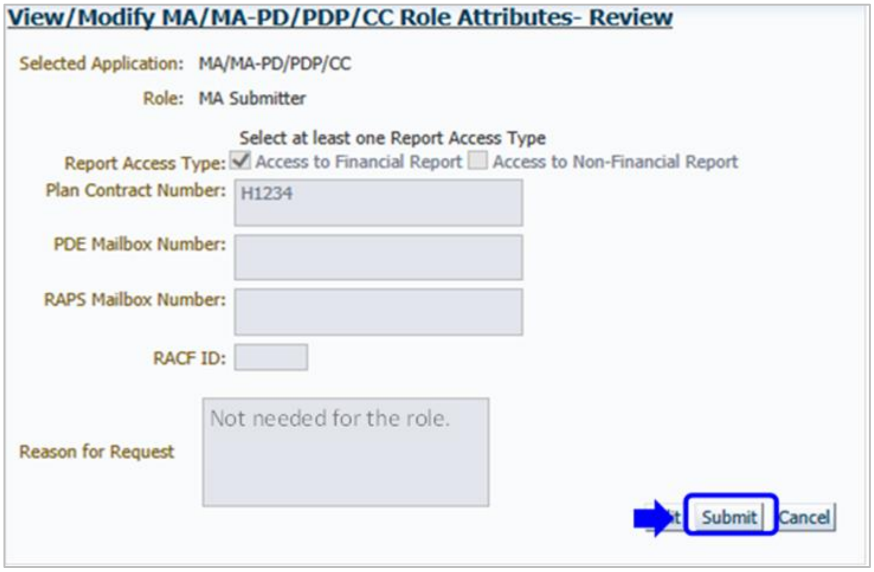


Step 12	After selecting **Next**, the **View/Modify Role Attributes - Review** page displays. Review the information displayed. Select **Edit** to modify the information. Select **Submit** to submit the request for approval.

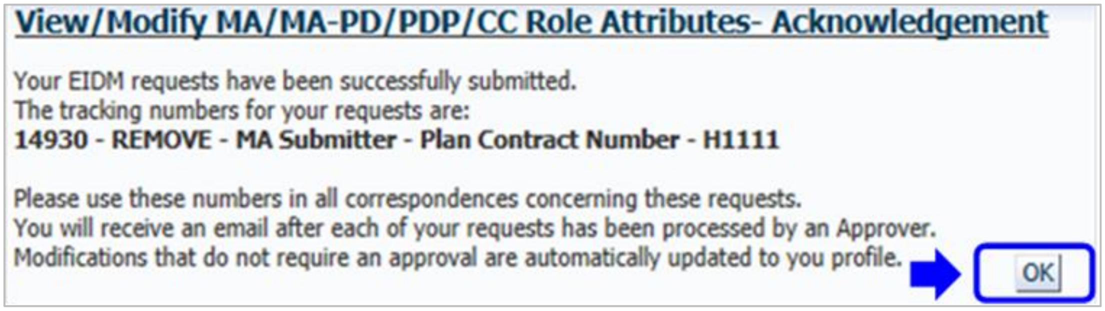
Note

You may select **Cancel** to exit out of the Remove a Role Attribute process. New information or changes entered do not save.

In the example below, the information is correct. Select **Submit**.



	Action
Step 13	After selecting Submit, the **View/Modify Role Attributes - Acknowledgement** page displays. The acknowledgement page displays the tracking number for the request, the role, and the role attributes to be removed. Select **OK** to close the acknowledgement page.



How to Replace an Existing Role with Another Role

The following is a quick overview on how to replace an existing role in an application with another role.

When you have an existing role *(e.g., an end user role, back-up security official, back-up authorized official, back-up approver)* and you need to replace your role with another role, for example, a higher-level role, you have to:

1. **Remove your existing role first**, and replace it with another role.
2. Submit a request for access for the new role.

To remove an existing role, follow the step-by-step instructions below.

To request access for a new role, or another role, follow the How to Request a Role

How to Remove a Role

The following are the basic step-by-step instructions on how to use the **Remove Role** feature to remove a role, when you are required to remove a role, and your application allows you to remove a role.

Important Note
If you are a DMEPOS Authorized Official and you have no people in your organization, you may use the Remove a Role feature to remove your role from the organization. Since you have no persons in your organization, your organization is also removed when EIDM completes the remove a role process. However, if you have persons that have been approved to access your DMEPOS organization, or you have pending requests for access for your organization, you are not able to remove your Authorized Official role. The reason: The persons in your organization, or applying for access, must have an Authorized Official in the organization.

To remove a DMEPOS Authorized Official role or any other role, please **FOLLOW THESE STEPS**:

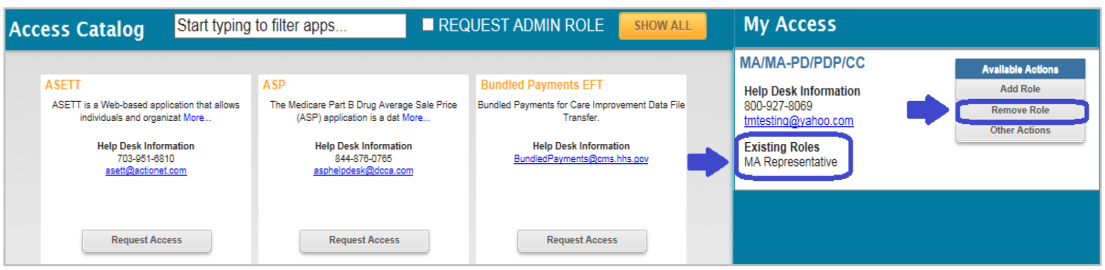
	Action
Step 1	Log into the CMS Enterprise Portal. Select the down arrow icon that appears next to your name at the top of page. Then select **My Access** from the drop-down list to continue. Alternately, you may select **Request Access Now** to continue.

Action

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

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

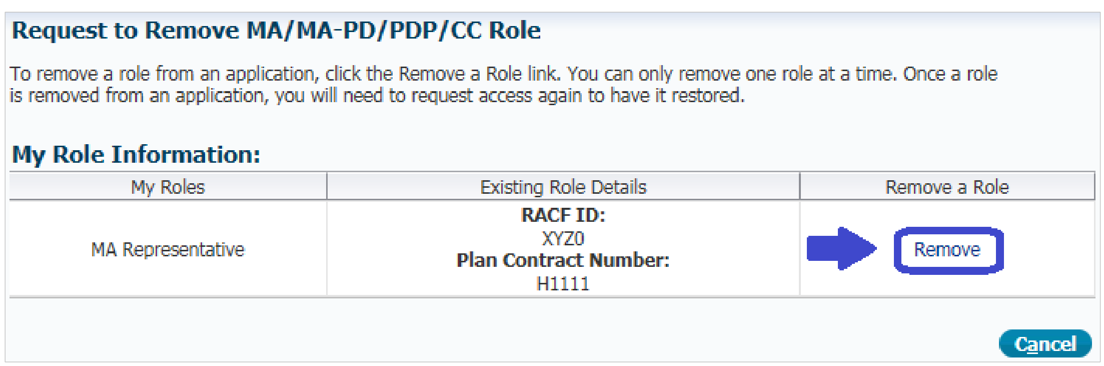
Select **Remove Role** for the application for which you are required to remove a role.



Step 3 The **Request to Remove Role** page displays.

All of your roles in the application are displayed in the **My Roles** section. All of your existing role details are displayed in the **Existing Role Details** section.

Select **Remove** for the role (backup security official, authorized official, service rep, end user, etc.) you wish to remove.

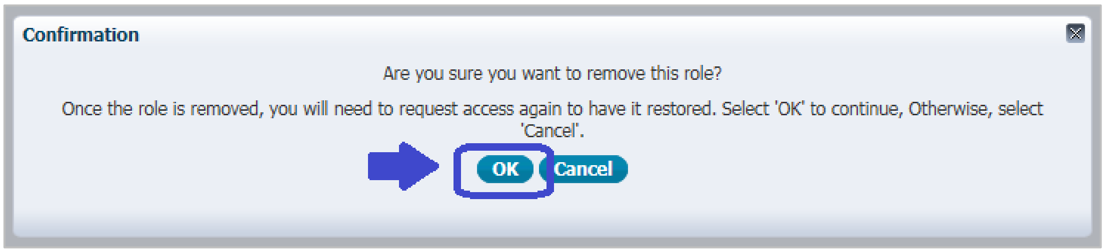


Action

Step 4 A confirmation message displays. The confirmation message asks “Are you sure you want to remove this role?” Review the confirmation message. Select **OK** to continue to remove the role. Select **Cancel** to stop the removal of the role.

Warning

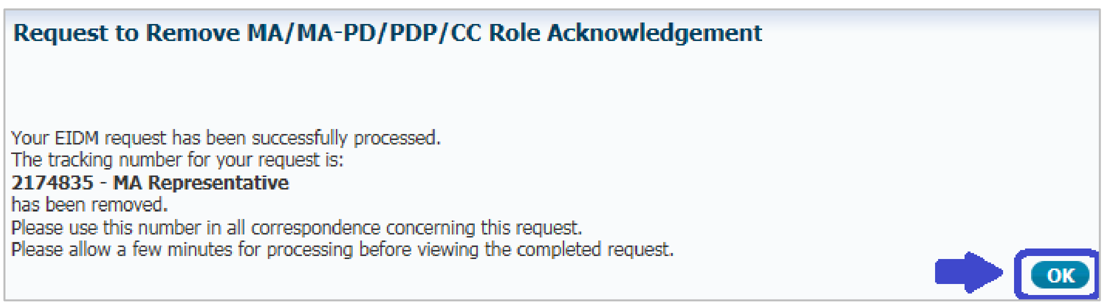
When you select **OK**, the role is removed at that time. You are not able to “undo” the removal.



Step 5 The **Request to Remove Role Acknowledgement** page displays.

The acknowledgement page displays the tracking number, for future correspondence, the role, and the role attribute or attributes that were removed.

Select **OK** to close the acknowledgement page.



Note

To request access to a new role, or another role, follow the Step-by-Step instructions on how to request access to an application and a role. Please allow a few minutes for processing the submitted request before requesting access to another role.

How to Add a Role

When you currently have a role in an application, and you are required to add another role in the same application, follow the step-by-step instructions below.

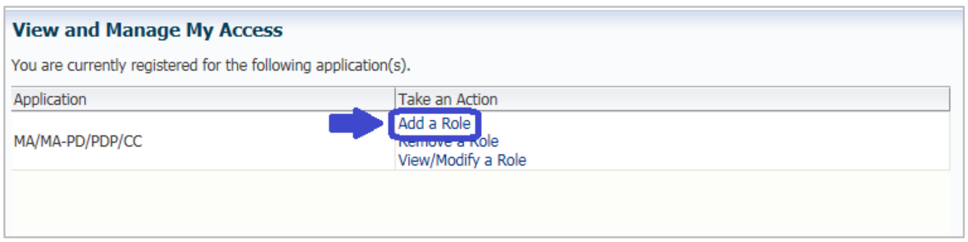
Important Note

If you currently do not have a role in the application, you have removed your role in the application, or your role has been removed, you need to request a role. Please see How to Request a Role.

The following are the basic step-by-step instructions on how to use the **Add a Role** feature when you already have a role in your application and your application allows you to add an additional role.

Action

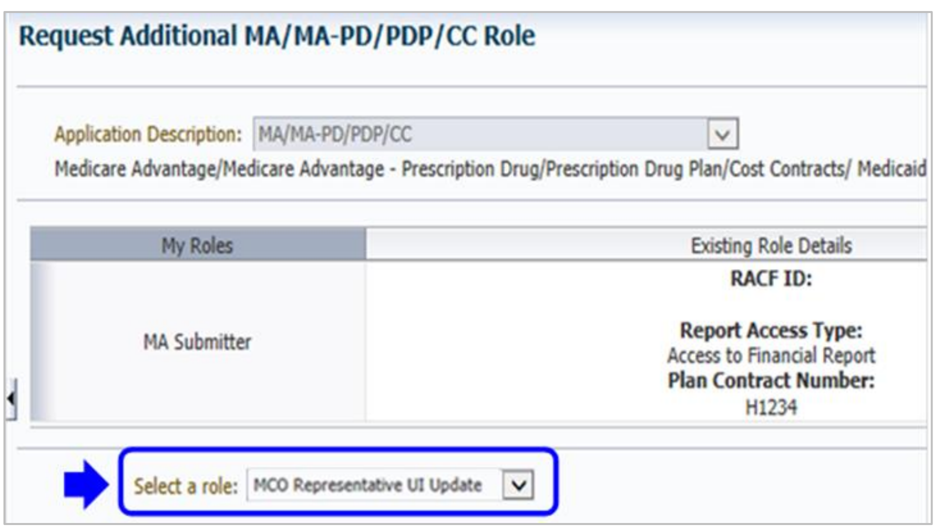
Step 1 After navigating to the **View and Manage My Access** page, select **Add a Role** for the application you are required to add a role.



Step 2 The **Request Additional Role** page displays.

All of your roles in the application are displayed in the **My Roles** section. All of your existing role details are displayed in the **Existing Role Details** section.

Select a role (security official, backup security official, authorized official, service rep, end user, etc.) from the **Select a role** drop-down list.



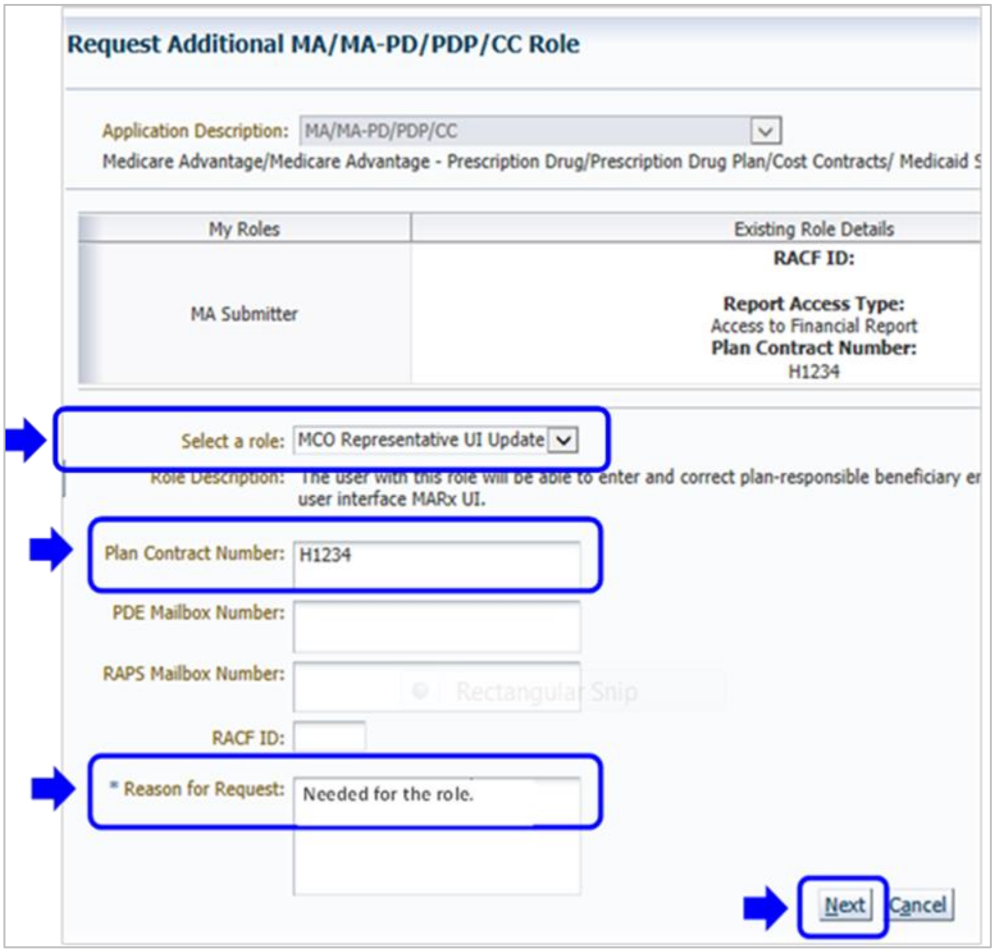
	Action
Step 3	The **Request Additional Role** page displays.

Provide the additional details needed for the role you are requesting, enter the reason for the request in the **Reason for Request** box.

Select **Next** to continue.

Note
You may select **Cancel** at any time to exit out of the Add a Role process. New information or changes entered do not save.

In the example below, we added **Plan Contract Number** H1234, entered the reason for the request in the **Reason for Request** box, and selected **Next** to continue.



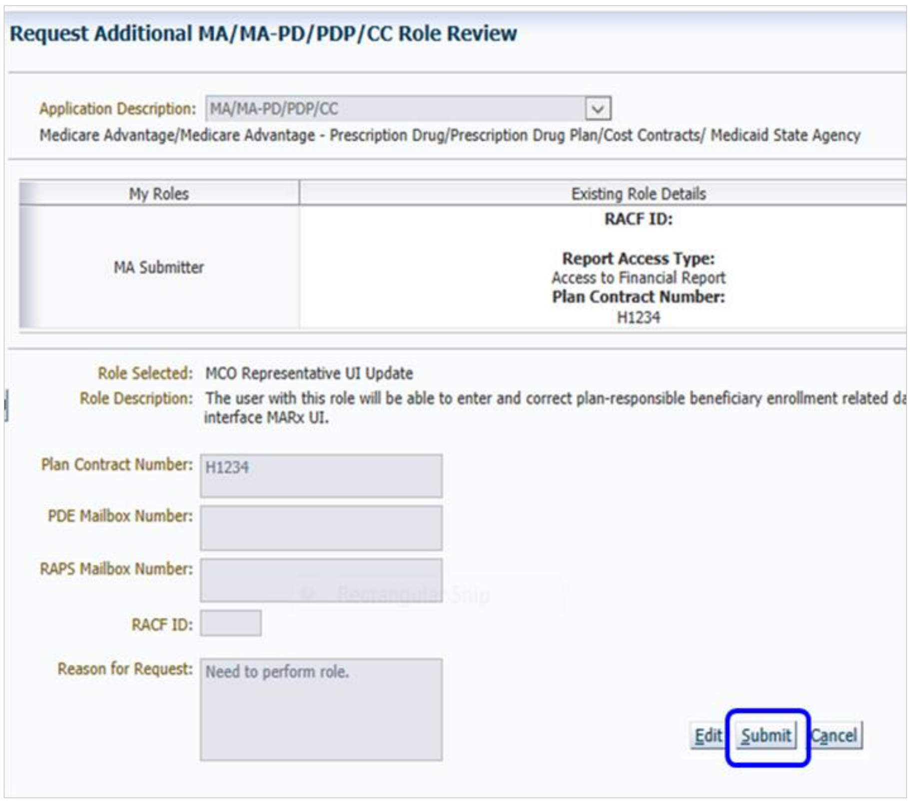
Action

Step 4 After selecting **Next**, the **Request Additional Role Review** page displays.

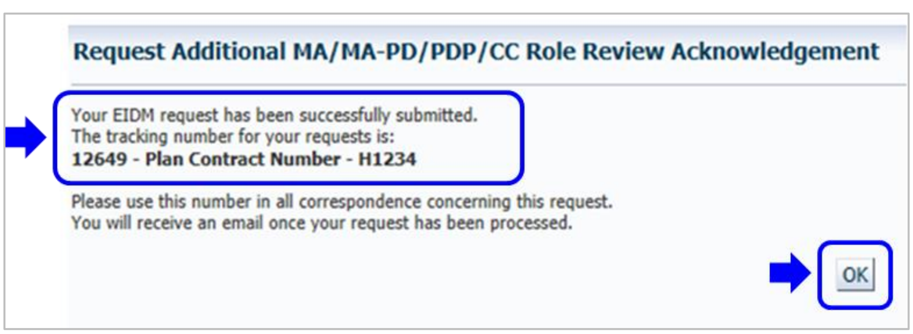
Review the information displayed. Select **Edit** to modify the information. Select **Submit** to submit the request for approval.

Note

You may select **Cancel** to exit out of the Add a Role process. New information or changes entered do not save.



Step 5 After selecting Submit, the **Request Additional Role Review Acknowledgement** page displays. It displays the tracking number for the request and the role attributes requested. Select **OK** to close the acknowledgement page.



How to Unlock Your Account

For security purposes, the system may lock your account because of any of the following circumstances:

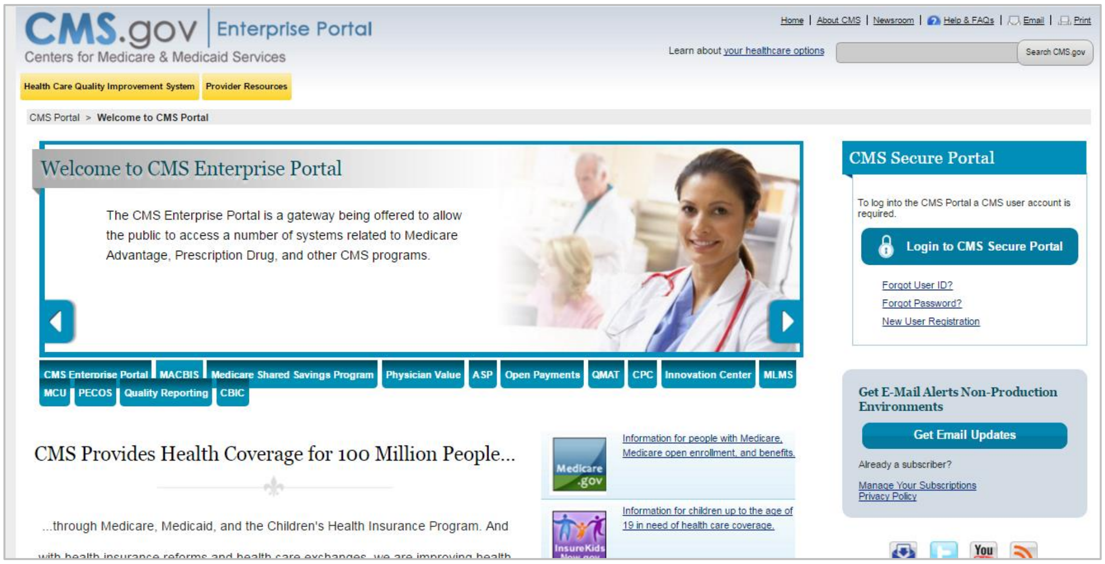
- The user has failed three consecutive login attempts.
- The user has failed three consecutive attempts at answering challenge questions.
- The user has not logged in for a specific number of days based on the security community to which the application role has been assigned (e.g., Provider Security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

If your account is locked and you attempt to login, you are redirected to the **Unlock My Account** page.

To unlock your account, **FOLLOW THESE STEPS**:

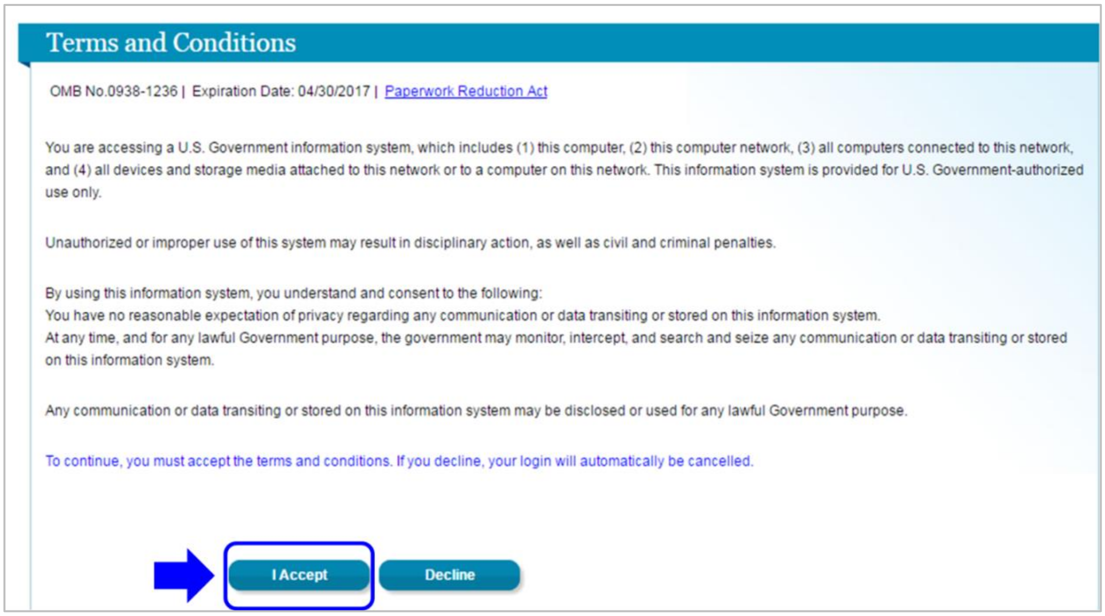
Action

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

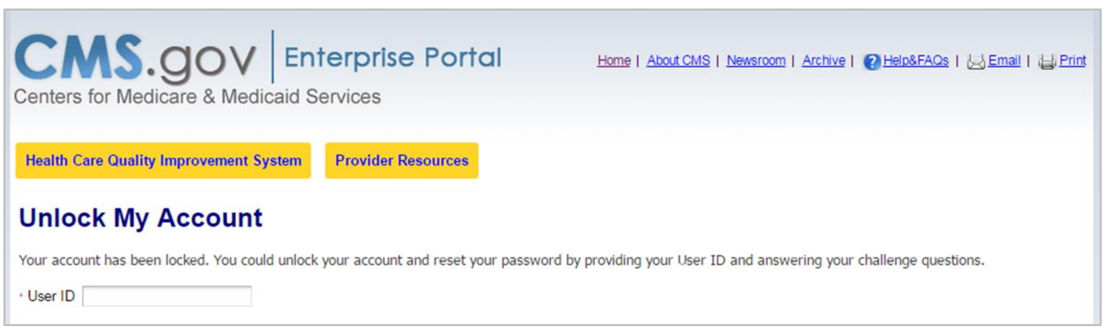


Step 2 Select **Login to CMS Secure Portal**.

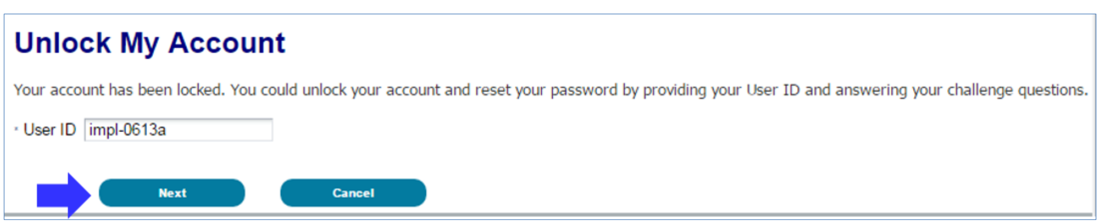
Action	
Step 3	Read the **Terms and Conditions** and select **I Accept** to continue.



Step 4	The **Unlock My Account** page displays.



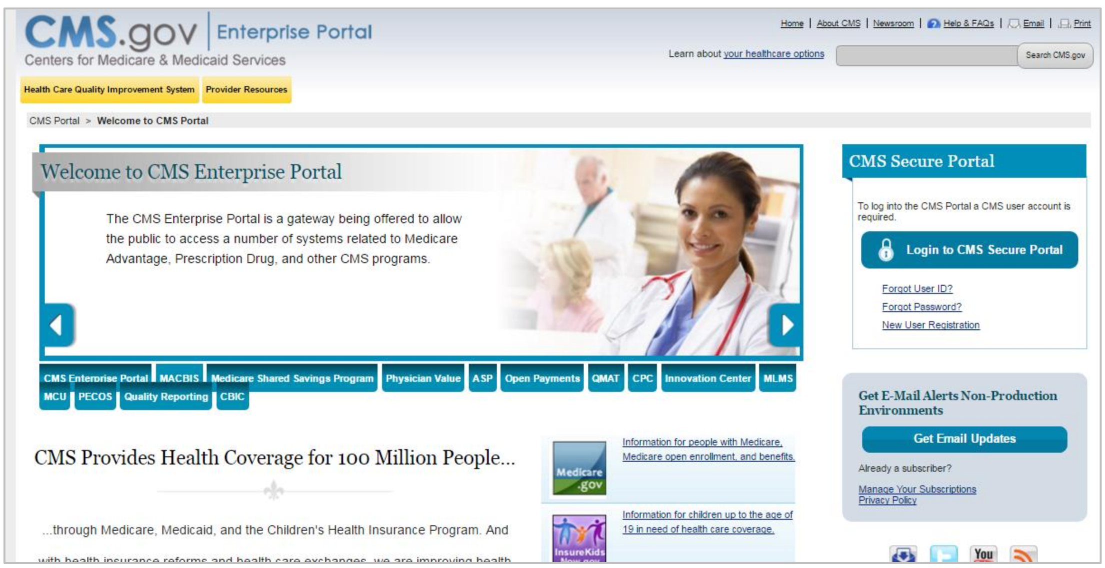
Step 5	Enter your **User ID** and select **Next**.



	Action
Step 6	Provide the answers to the challenge questions displayed. Enter a new password and select **Next**.

Step 7	Then **Unlock My Account** acknowledgement page displays. The page displays that your account has been unlocked successfully. Select **Next.**

The **CMS Enterprise Portal** page displays for you to log into your account.



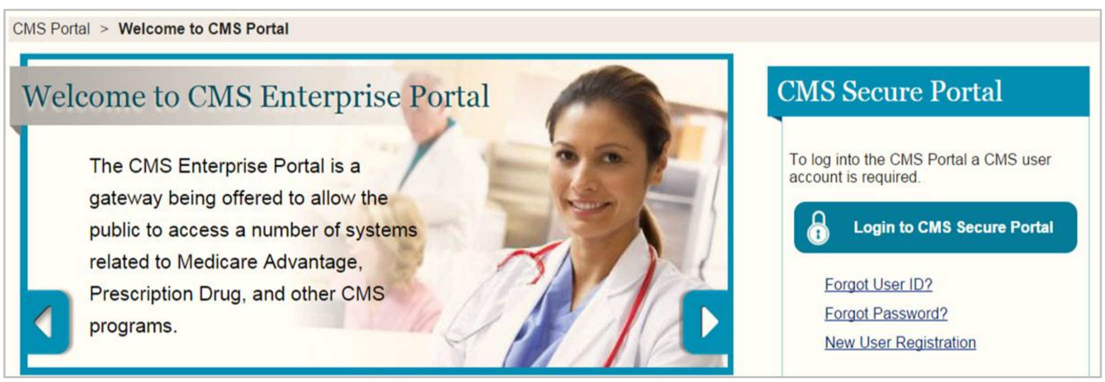
8. Changing Your User Profile

This section provides assistance and basic step-by-step instructions for the following:

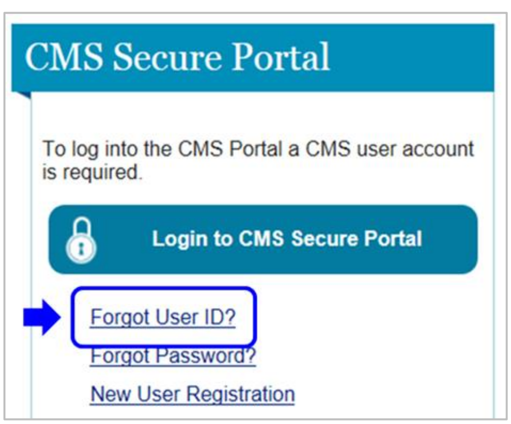
Forgot Your User ID?

The following are the basic step-by-step instructions on how to use the **Forgot User ID?** feature.

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



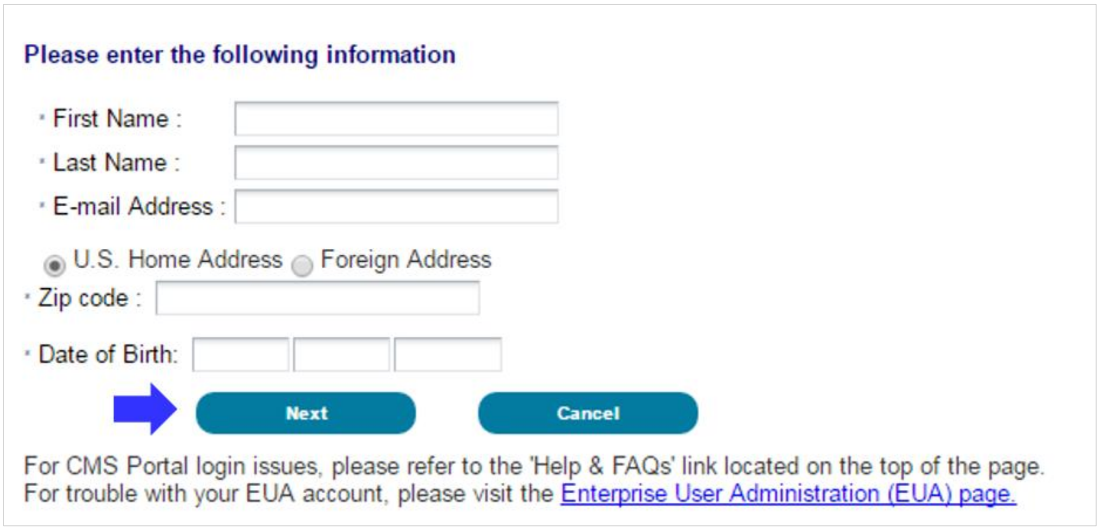
Step 2	Select the **Forgot User ID?** link.



Action

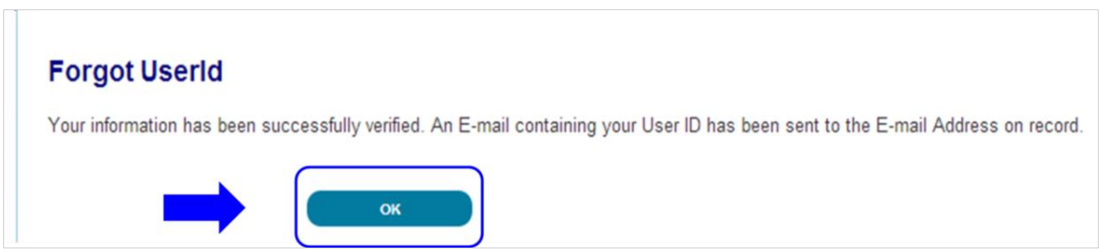
Step 3 Provide the information requested and select **Next** to continue.

> **Note**
>
> You may select **Cancel** at any time to exit out of the **Forgot User ID** process. New information or changes entered do not save.



Step 4 After selecting **Next**, the **Forgot User ID** acknowledgement page displays. The page displays that the information entered has been verified and an e-mail, with your User ID, has been sent to the e-mail address on record.

Select **OK** to close the page.

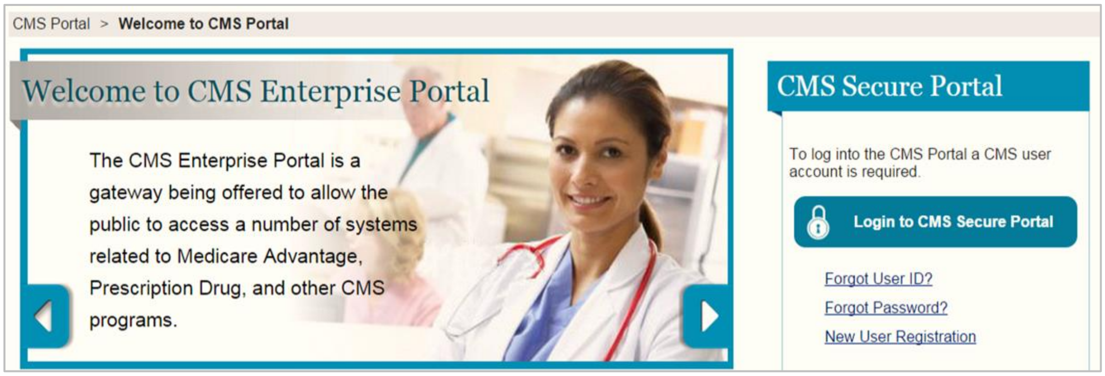


Forgot Your Password?

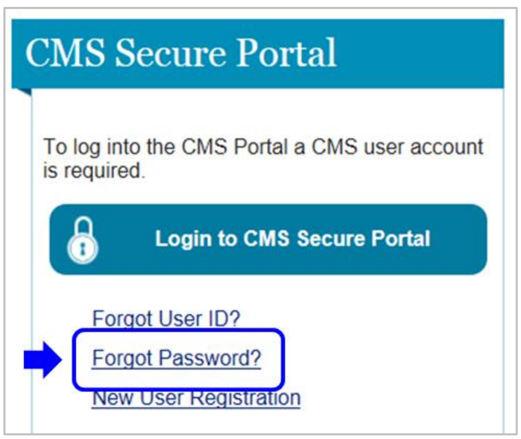
The following are the basic step-by-step instructions on how to use the **Forgot Password?** feature to create a new password.

Action

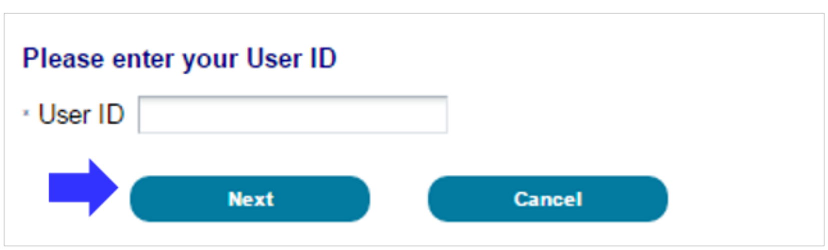
Step 1 Navigate to https://portal.cms.gov. The **CMS Enterprise Portal** page displays as illustrated below.



Step 2 Select the **Forgot Password?** link.



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



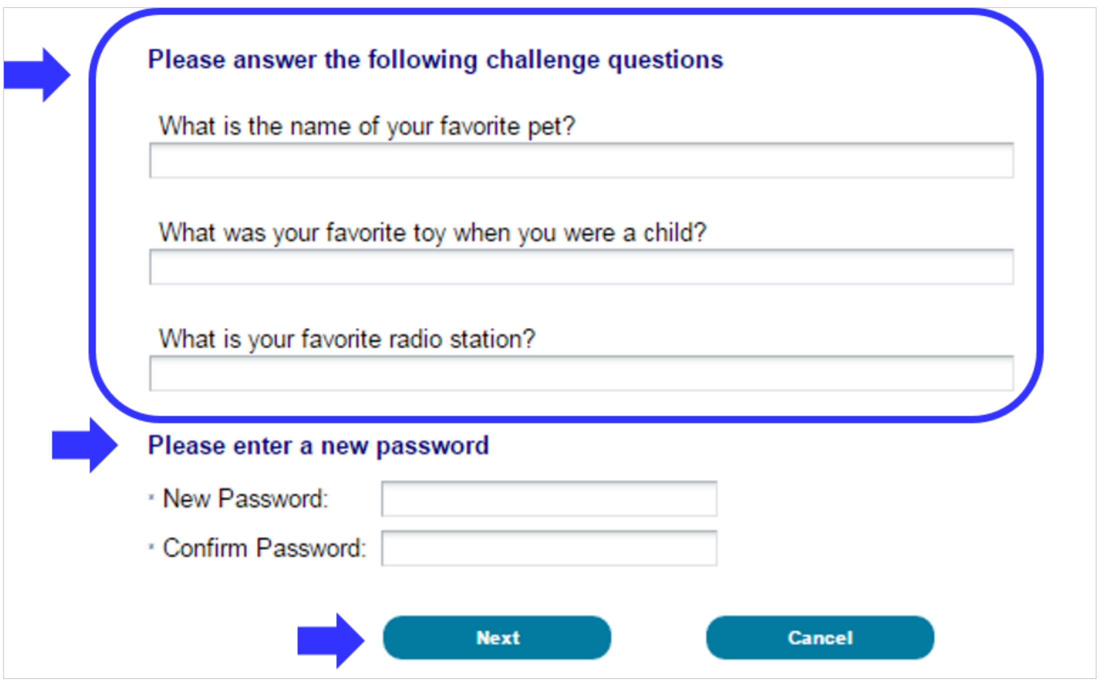
Action

Step 4 Provide the answers to the challenge questions displayed.

Enter a new password. Re-enter the same password for “**Confirm Password**” and select **Next** to complete the Forgot Password process.

Notes

- EIDM displays instructions on what you are required to include in your password.
- Passwords must not contain any commonly used words or phrases that are 3 characters or more in length, such as “love”, “June”, “123”, etc.
- Some roles may require you to enter an 8-character password for your new password. For example, if you have a role in an application where a CMS 4-character Resource Access Control Facility (RACF) is used for identification and verification, you may have to create and enter an 8-character password for your new password. When you are required to enter an 8-character password, an error message displays when a password has been entered that is longer than 8 characters.



Step 5 After selecting **Next**, the **Forgot Password** acknowledgement page displays. The page displays that the password has been changed and a confirmation e-mail has been sent to the e-mail address on record.

Select **OK** to close the page.

Note

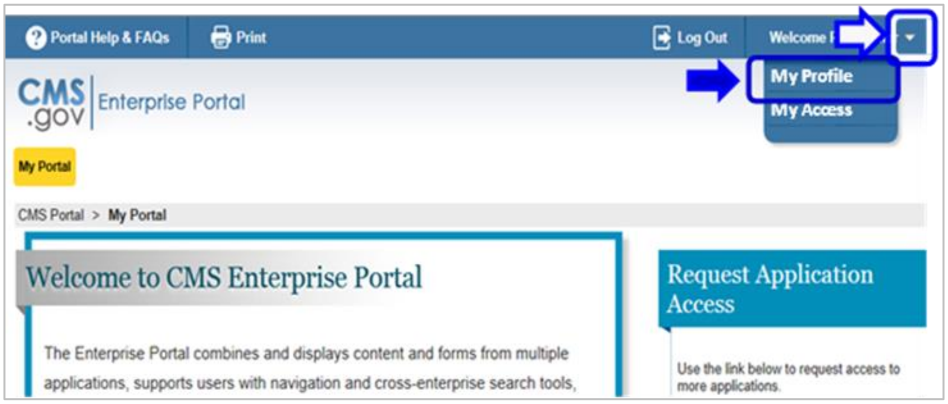
You may select **Cancel** at any time to exit out of the Forgot Password process. New information or changes entered do not save.

Action
Forgot Password Your password has been successfully changed. A confirmation E-mail has been sent. OK

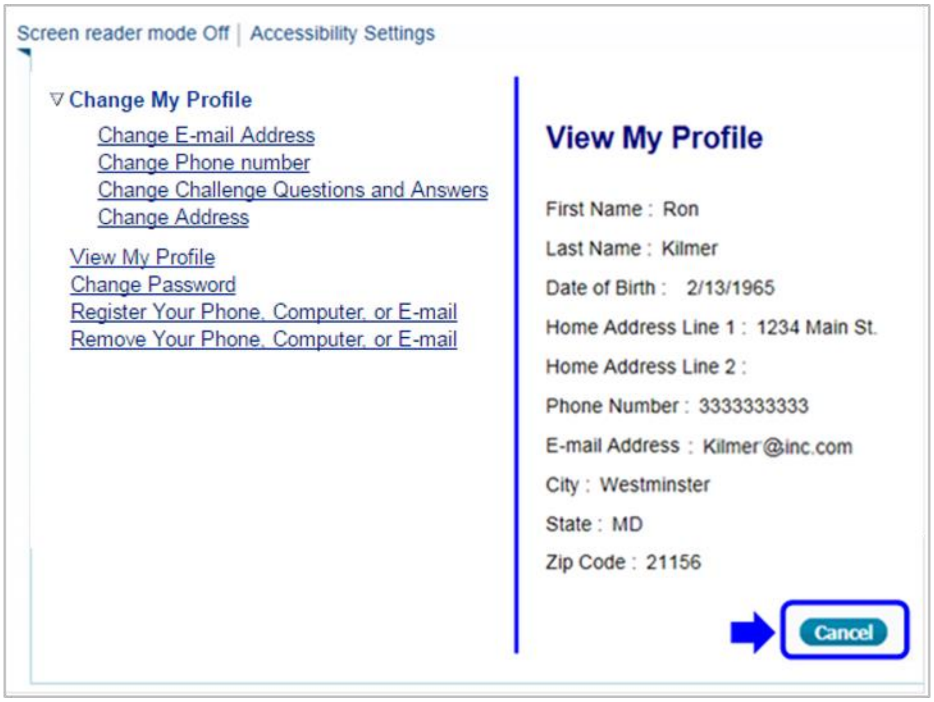
How to View Your Profile

The following are the basic step-by-step instructions on how to use the **View My Profile** feature to view your profile information.

	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 Profile** from the drop-down list to continue.

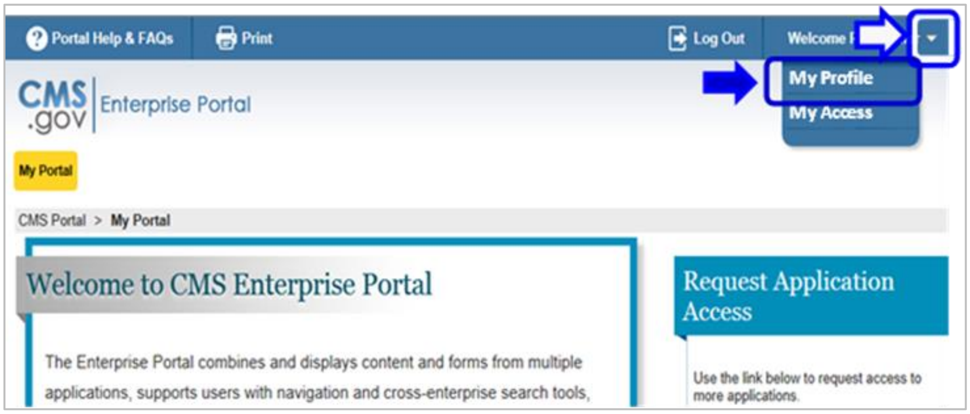
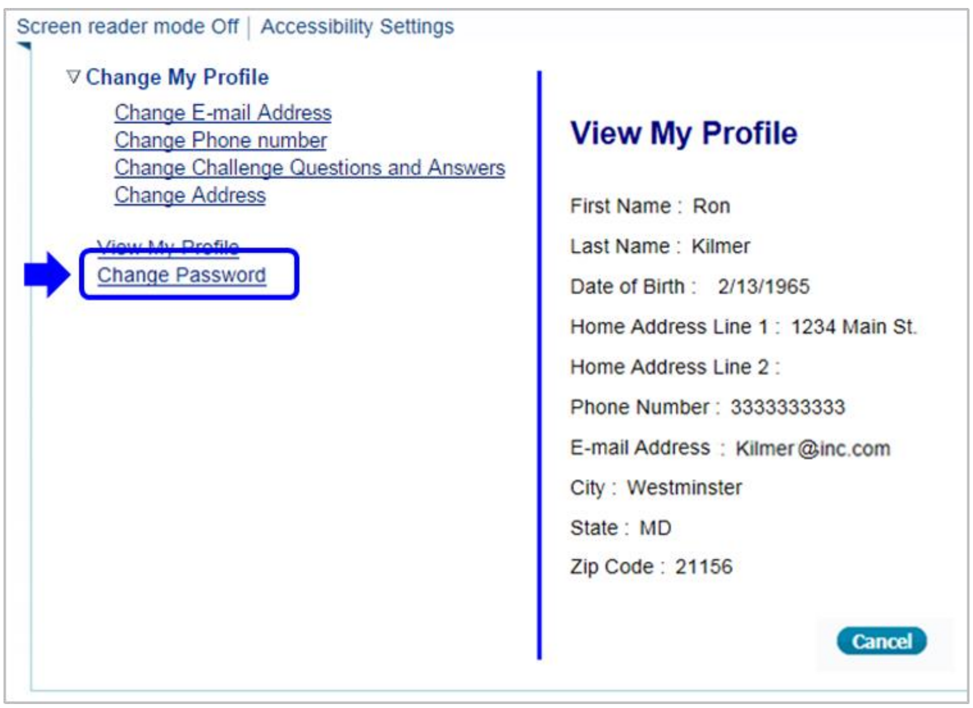


Step 2	The **View My Profile** page displays. After viewing your profile information, select **Cancel** to close the page.



How to Change Your Password

The following are the basic step-by-step instructions on how to use the **Change Password** feature to change your password.

	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 Profile** from the drop-down list to continue. 
Step 2	The **View My Profile** page displays. Select **Change Password**. 

Action

Step 3 The **Change Password** page displays.

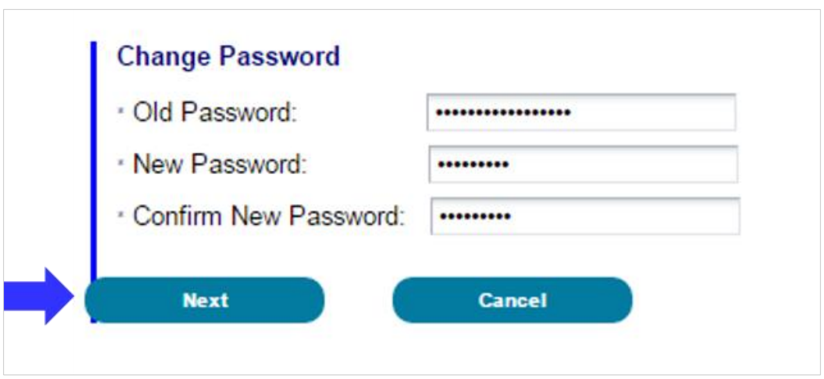
Enter your old password.

Create and enter a new password of your choice in the **New Password** field.

Re-enter the same password in the **Confirm Password** field and select **Next** to continue.

Notes

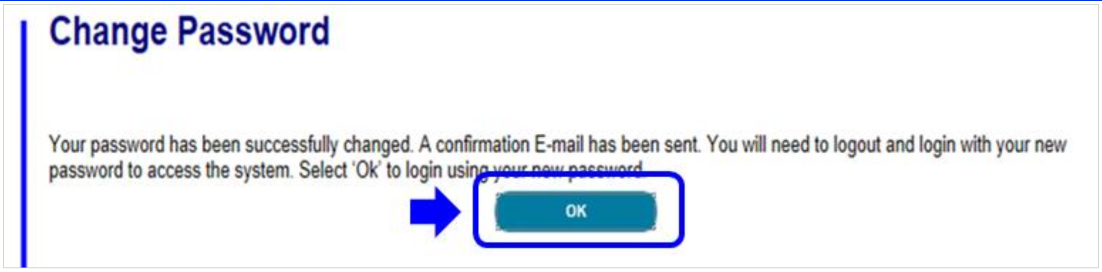
- EIDM displays instructions on what you are required to include in your password. Passwords must not contain any commonly used words or phrases that are 3 characters or more in lenght such as “love”, “June”, “123” etc.
- Passwords must not contain any commonly used words or phrases that are 3 characters or more in length, such as “love”, “June”, “123”, etc.
- Some roles may require you to enter an 8-character password for your new password. For example, if you have a role in an application where a CMS 4-character Resource Access Control Facility (RACF) is used for identification and verification, you may have to create and enter an 8-character password for your new password. When you are required to enter an 8-character password, an error message displays when a password has been entered that is longer than 8 characters.
- You may select Cancel at any time to exit out of the Change Password process. New information or changes entered do not save.



Step 4 The **Change Password** acknowledgement page displays.

It shows that the password has been changed, a confirmation e-mail has been sent to the e-mail address on record, and you need to logout and login with your new password.

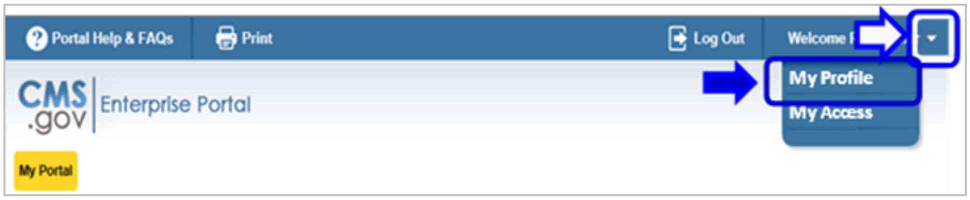
Select **OK** to close the page.

Action
Change Password Your password has been successfully changed. A confirmation E-mail has been sent. You will need to logout and login with your new password to access the system. Select 'Ok' to login using your new password. OK

How to Change Your E-mail Address

The following are the basic step-by-step instructions on how to use the **Change E-mail Address** feature to change your e-mail address.

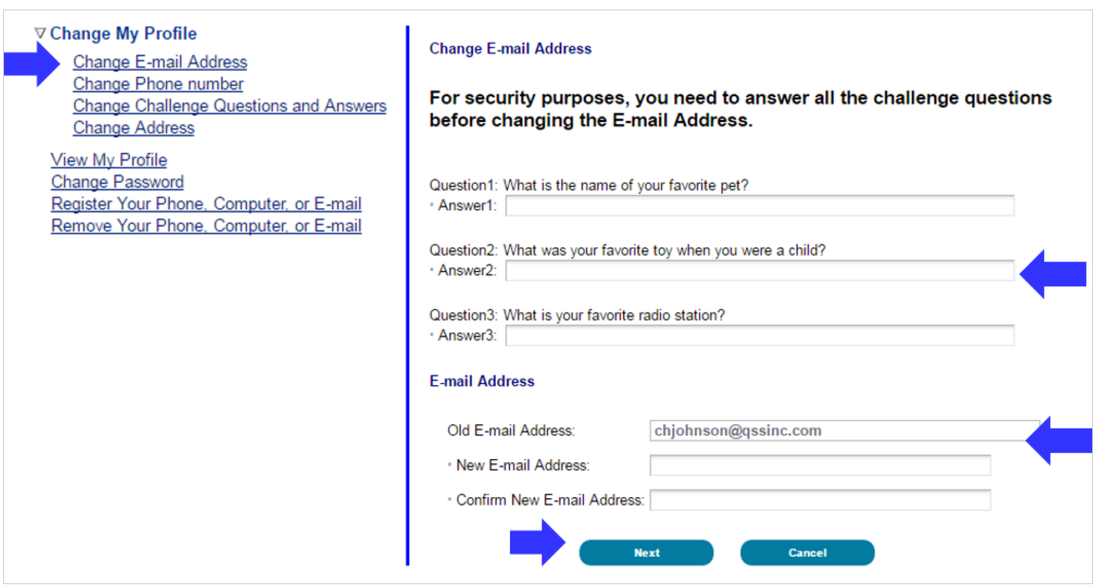
	Action
Step 1	Log into the CMS Enterprise Portal. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.

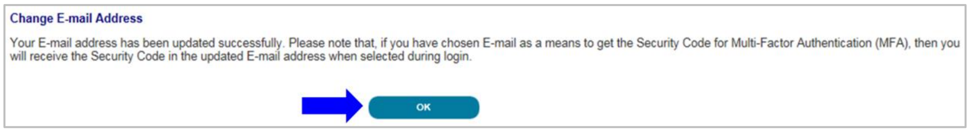


Step 2	The **View My Profile** page displays. Select **Change E-mail Address**. Provide the answers to the challenge questions displayed. Enter your new e-mail address in the **New E-mail Address** field and then re-enter the e-mail address in the **Confirm New E-mail Address** field. Select **Next** to complete the Change e-mail process.

Note

You may select **Cancel** at any time to exit out of the Change Password process. New information or changes entered do not save.



	Action
Step 3	The **Change E-mail Address** acknowledgement page displays. It shows that the e-mail address has been changed. In addition, the system sends a confirmation e-mail to both the old and new addresses. Select **OK** to close the page. 

How to Change Your Security Challenge Questions and Answers

The following are the basic step-by-step instructions on how to use the **Change Challenge Questions and Answers** feature to change your security challenge questions and answers.

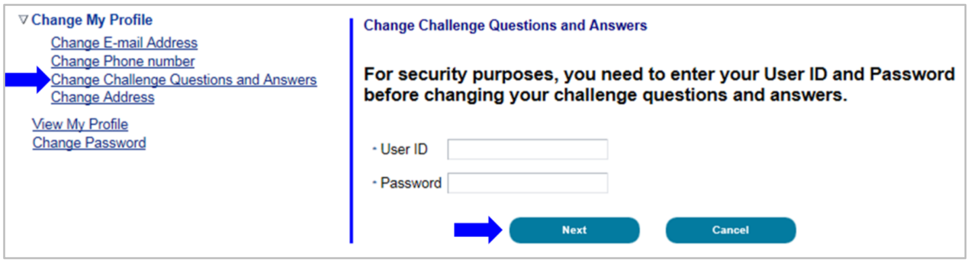
Action

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 Profile** from the drop-down list to continue.

Step 2 The **View My Profile** page displays.

Select **Change Challenge Questions and Answers**. Enter your **User ID** and **Password** and select **Next**.

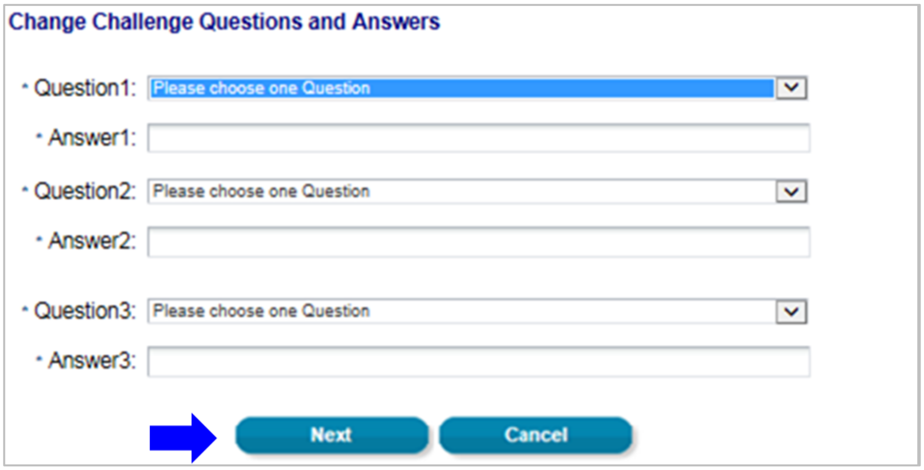


Step 3 The **Change Challenge Questions and Answers** page displays.

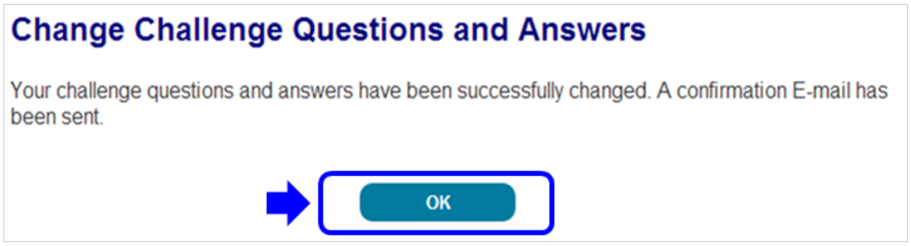
Select a question and then provide an answer of your choosing. Continue until all three challenge questions have been selected and answered. Select **Next**.

Note

You may select **Cancel** at any time to exit out of the Change Challenge Questions process. New information entered do not save.

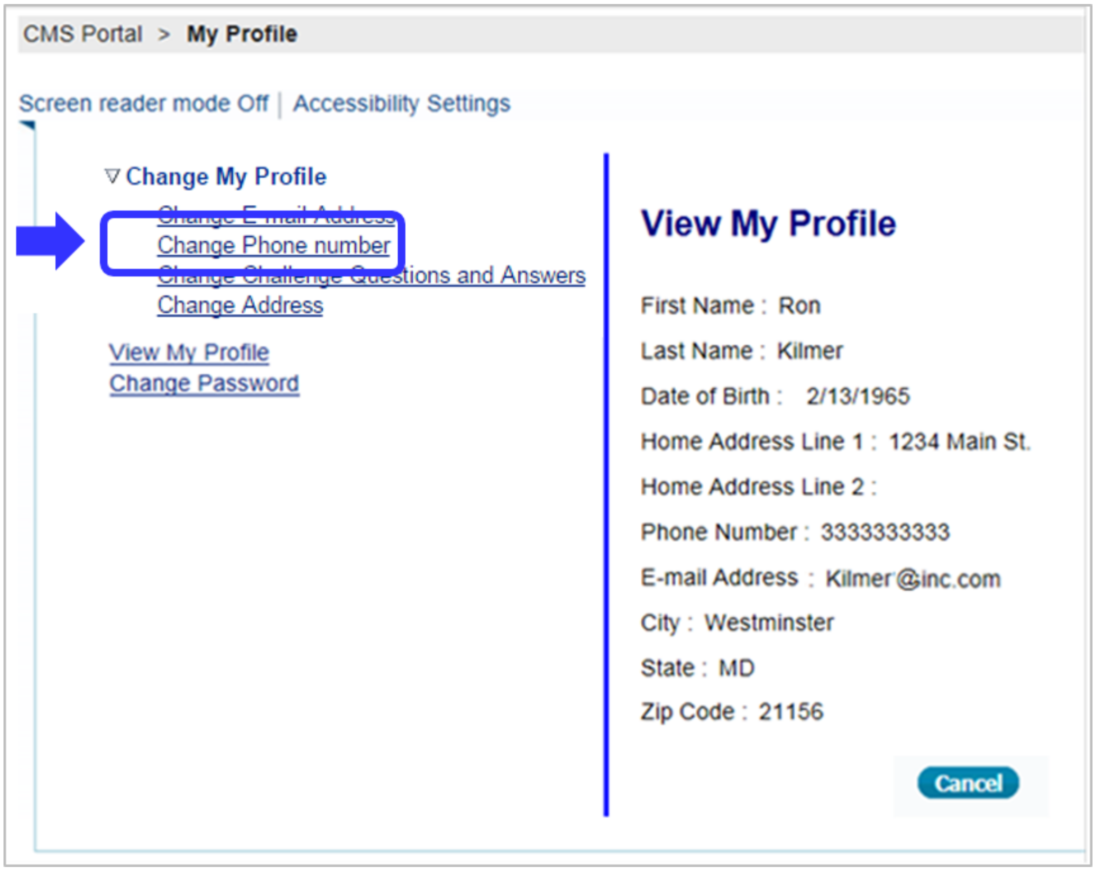


	Action
Step 4	The **Change Challenge Questions and Answers** acknowledgement page displays. It shows that the challenge questions and answers have been changed and a confirmation e-mail has been sent to the e-mail address on record. Select **OK** to close the page.



How to Change Your Phone Number

The following are the basic step-by-step instructions on how to use the **Change Phone number** feature to change your phone number.

	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 Profile** from the drop-down list to continue. 
Step 2	The **View My Profile** page displays. Select **Change Phone number**. 

	Action
Step 3	The **Change Phone number** page displays.

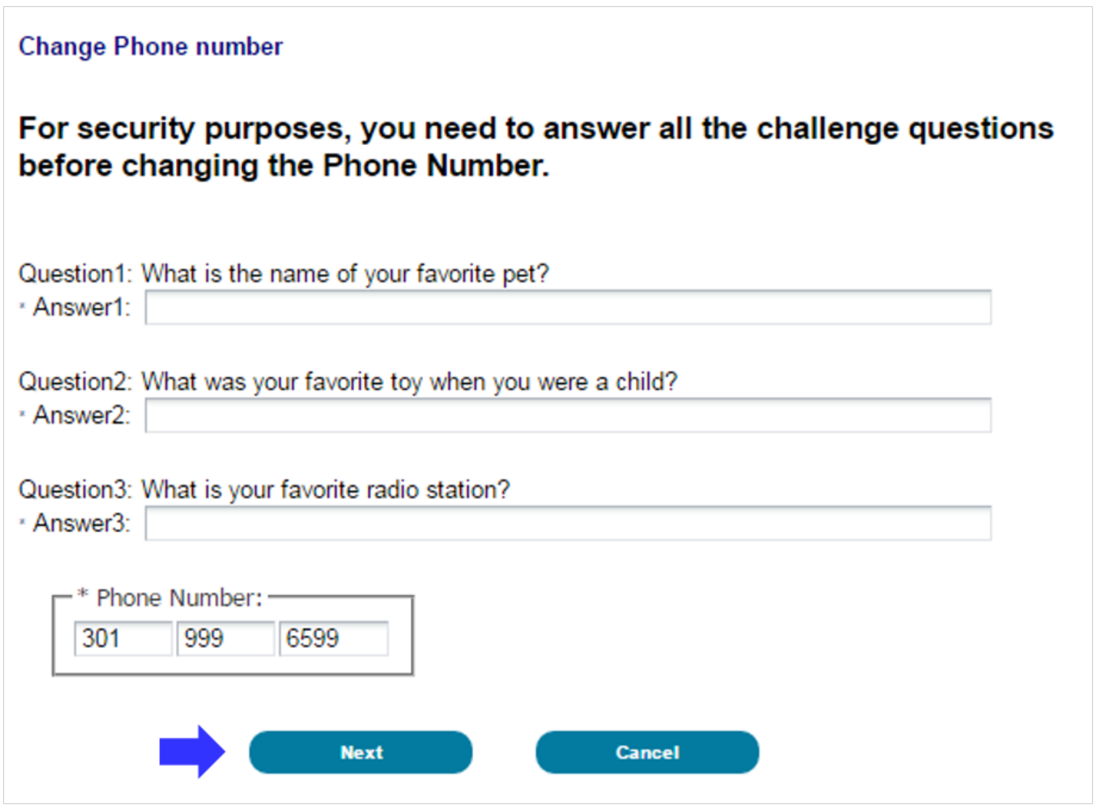
The current phone number on record for you displays in the **Phone Number** field.

Provide the answers to all of the challenge questions displayed.

Enter your new phone number in the Phone Number field.

Select **Next** to continue.

Note
You may select **Cancel** at any time to exit out of the Change Phone number process. New information or changes entered do not save.

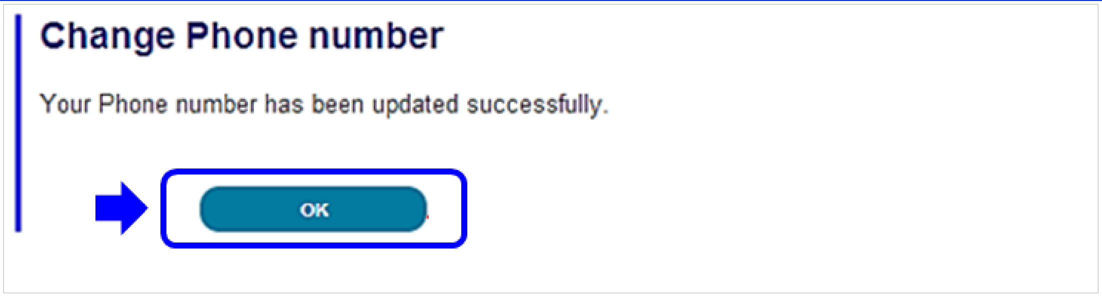


Step 4	The **Change Phone number** acknowledgement page displays.

It shows that the phone number has been changed. In addition, the system sends a confirmation e-mail to the address on record.

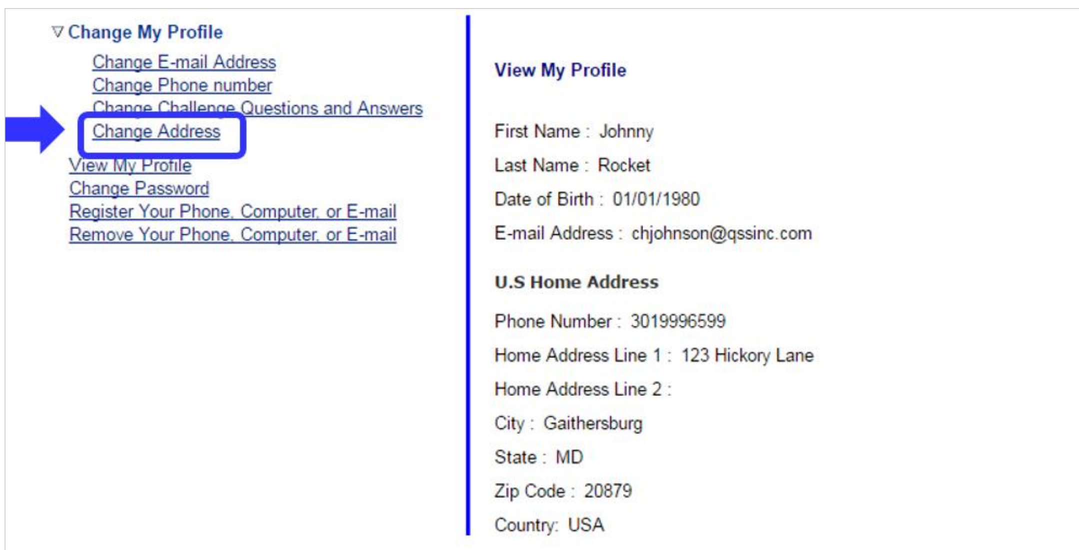
Select **OK** to close the page.

Action


Change Phone number
Your Phone number has been updated successfully.
OK

How to Change Your Address

The following are the basic step-by-step instructions on how to use the **Change Address** feature to change your address.

	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 Profile** from the drop-down list to continue. 
Step 2	The **View My Profile** page displays. Select **Change Address**. 

Action

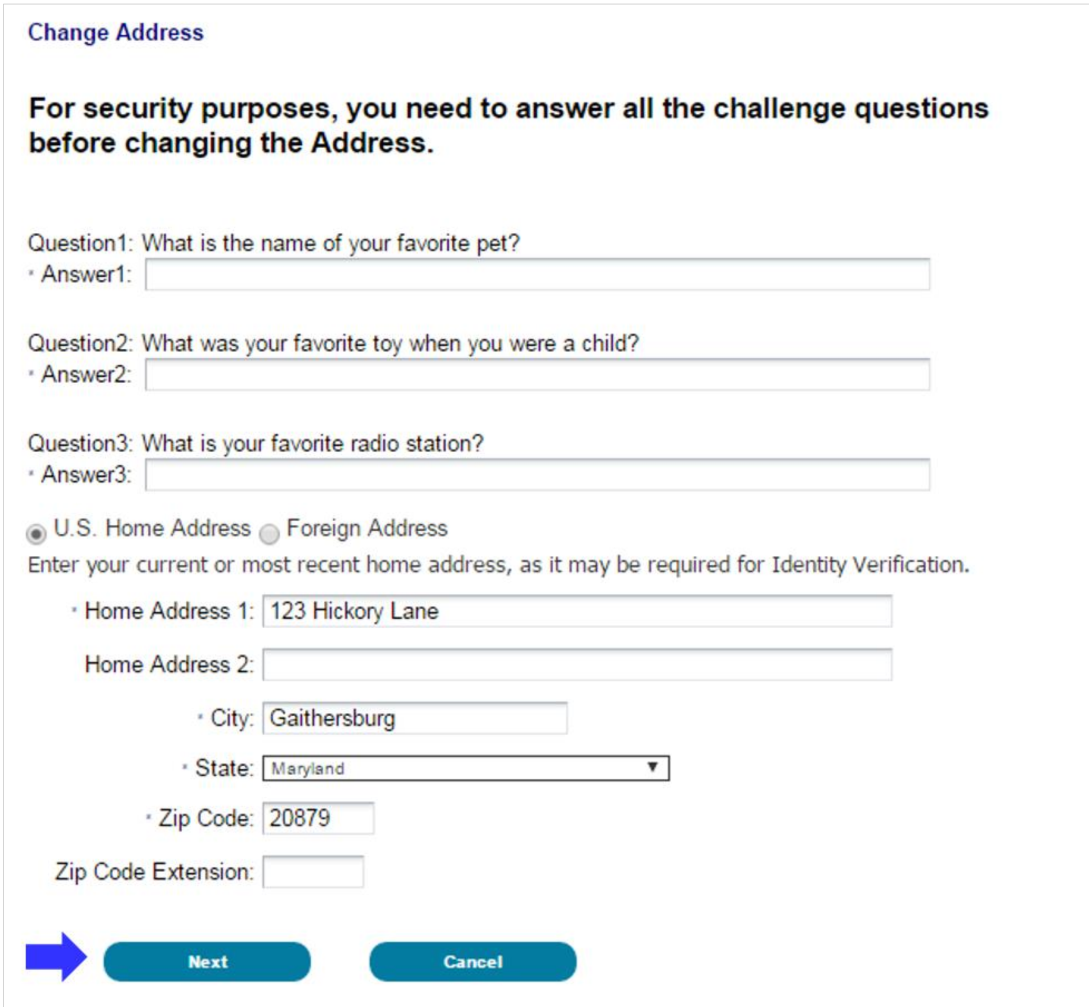
Step 3 The **Change Address** page displays.

The current address on record displays in the **Address** field. Provide the answers to all of the challenge questions displayed.

Enter your new address information in the **Address** field.

Select **Next** to complete the **Change Address** process.

> **Note**
>
> You may select **Cancel** at any time to exit out of the Change Address process. New information or changes entered do not save.



Step 4 The **Change Address** acknowledgement page displays.

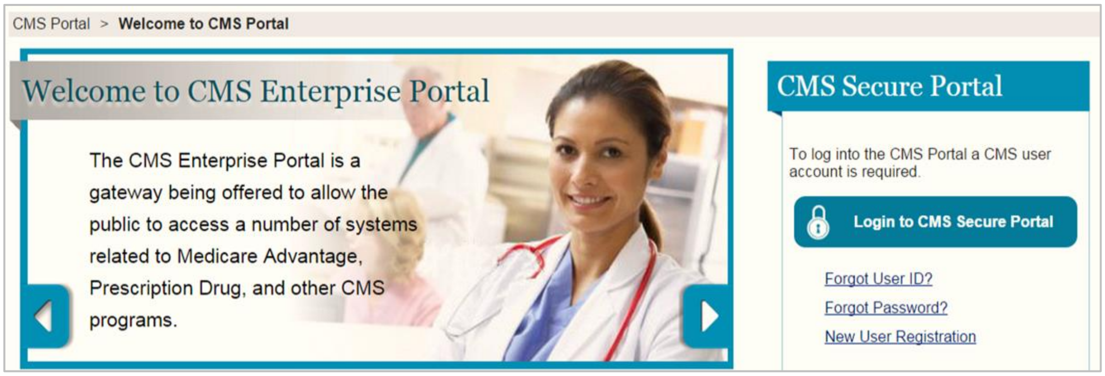
It shows that the address has been changed. In addition, the system sends a confirmation e-mail to the address on record.

Select **OK** to close the page.

How to Change an Expired Password

The following are the basic step-by-step instructions on how to use the **Change Expired Password** feature to reset an Expired Password.

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

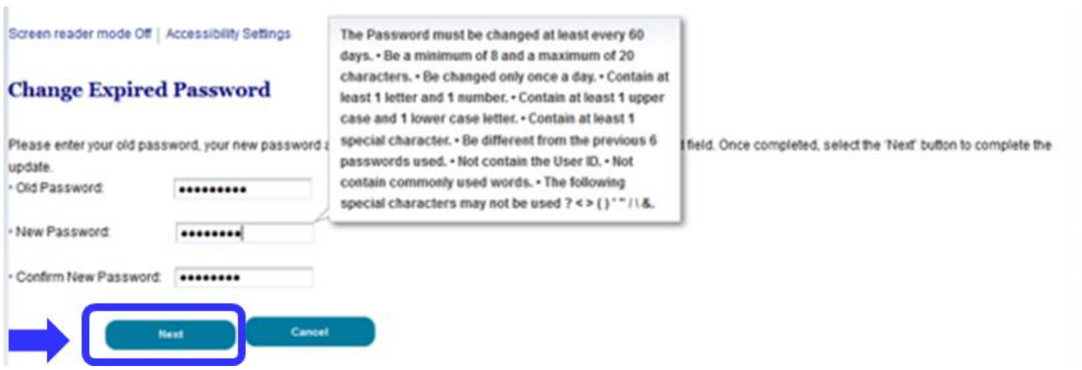


Step 2	Select **Login to CMS Secure Portal**.

	Action
Step 3	Enter your old password and a new password. Re-enter the same password for "**Confirm New Password**" and select **Next** to complete the Forgot Password process.

Note

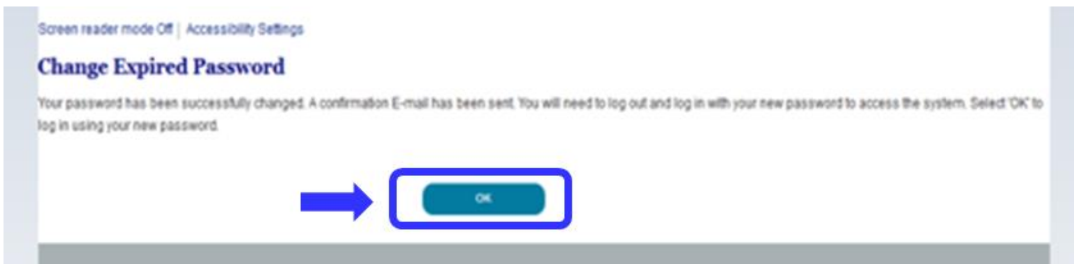
- EIDM displays instructions on what you are required to include in your password.
- Passwords must not contain any commonly used words or phrases that are 3 characters or more in length, such as "love", "June", "123", etc.
- Some roles may require you to enter an 8-character password for your new password. For example, if you have a role in an application where a CMS 4-character Resource Access Control Facility (RACF) is used for identification and verification, you may have to create and enter an 8-character password for your new password. When you are required to enter an 8-character password, an error message displays when a password has been entered that is longer than 8 characters.



Step 4	After selecting **Next**, the **Change Expired Password** acknowledgement page displays. The page indicates that the password has been changed and a confirmation e-mail has been sent to the e-mail address on record. Select **OK** to close the page.

Note

You may select **Cancel** at any time to exit out of the Change Expired Password process. New information or changes entered do not save.



9. User initiated Annual Certification

When a user's role request is approved, that role is granted to the user for one year. Continued use of the role must be approved, or "certified" each year by the designated approver for that role. Users have the option of notifying their approvers of the continued need for their roles by selecting the "Annual Certification" link on their profile page. Notifying your approver helps ensure that the annual certification of that role is completed in a timely manner and without interruption.

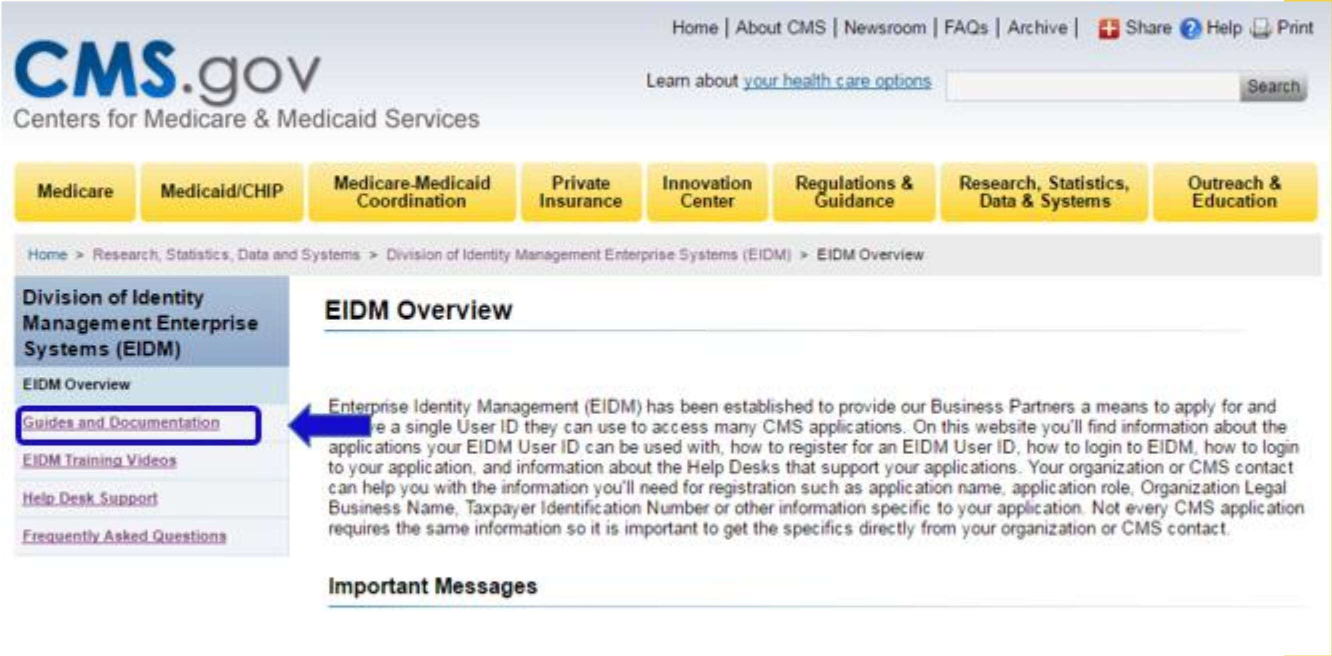
This process is initiated with an E-mail notification to the End Users:

1. An End User with a manually approved role will receive E-mail notifications on a biweekly basis on the first and fifteenth of every month if they have not submitted their role(s) for Annual Certification. The notifications begin when the certification due date is within 45 days of the e-mail notification period.
2. The E-mail notifies the End User that his role is due for Annual Certification along with the instructions to submit the role for recertification or to remove the role, if they no longer need the role.
3. The End User can login to EIDM and select the role they wish to recertify via the **My Annual Certifications View** page and submits the request. Upon submission of this request, the status of the role request is set to **Submitted** in the My Annual Certifications View page. The End User can also remove the role via the **View and Manage My Access** page.
4. The role status is updated to **Certified** when the approver recertifies the role.
5. The End User will receive an E-mail when the approver certifies/revokes the role or if no action is taken by the certification due date.

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.

For more detailed instructions, please refer to Section 3: User Initiated Annual Certification in the EIDM Quick Reference Guide entitled: "*Completing Annual Certification*". EIDM Quick Reference Guides can be accessed in the Guides and Documentation section of the EIDM Overview page as show below.



Home | About CMS | Newsroom | FAQs | Archive | Share Help Print
CMS.gov
Centers for Medicare & Medicaid Services
Learn about your health care options
Search
Medicare
Medicaid/CHIP
Medicare-Medicaid Coordination
Private Insurance
Innovation Center
Regulations & Guidance
Research, Statistics, Data & Systems
Outreach & Education
Home > Research, Statistics, Data and Systems > Division of Identity Management Enterprise Systems (EIDM) > EIDM Overview
Division of Identity Management Enterprise Systems (EIDM)
EIDM Overview
Guides and Documentation
EIDM Training Videos
Help Desk Support
Frequently Asked Questions
EIDM Overview
Enterprise Identity Management (EIDM) has been established to provide our Business Partners a means to apply for and
e a single User ID they can use to access many CMS applications. On this website you'll find information about the
applications your EIDM User ID can be used with, how to register for an EIDM User ID, how to login to EIDM, how to login
to your application, and information about the Help Desks that support your applications. Your organization or CMS contact
can help you with the information you'll need for registration such as application name, application role, Organization Legal
Business Name, Taxpayer Identification Number or other information specific to 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.
Important Messages

10. 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
	Does the account have a role?	Yes	Account review passes. No further action is taken.
		No	Proceed to next step.
1.	Has the account been inactive for less than 180 days?	Yes	Account review passes. No further action is taken.
		No	Proceed to next step.
2.	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.
3.	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

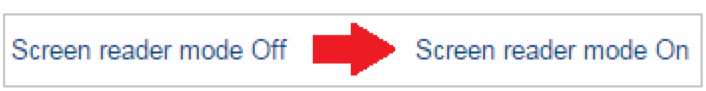
The E-mail includes instructions to regain access to the CMS Enterprise Portal by registering for a new user account.

11. Appendices

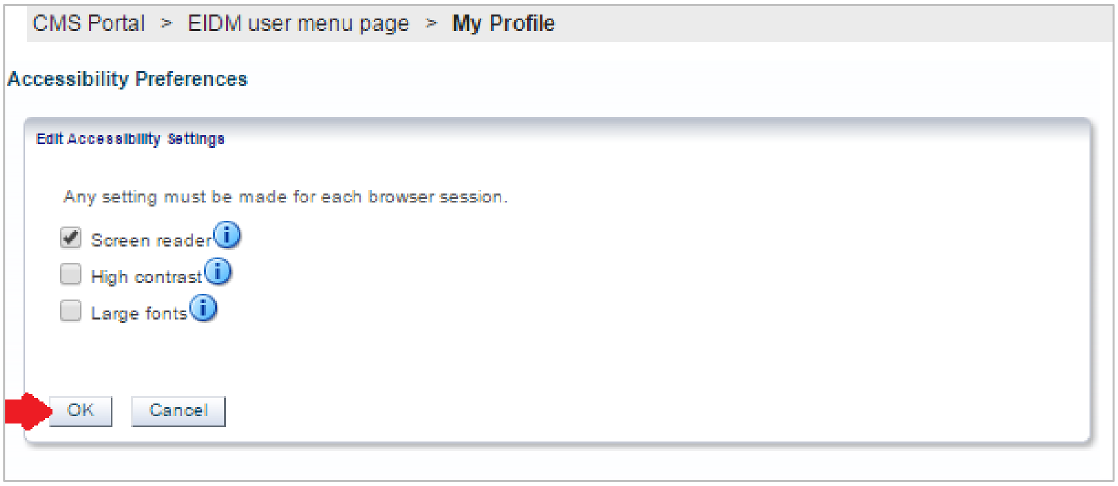
Appendix A: Accessing EIDM in 508 Accessibility Mode

Section 508 is a federal law that requires agencies to provide people with disabilities equal access to electronic information and data comparable to those who do not have disabilities, unless doing so would impose an undue burden on the agency. The Section 508 standards are the technical requirements and criteria used to determine whether the agency is meeting the requirements of this law.

This section outlines the steps users can take to access EIDM in 508 Accessibility Mode.

	Action
Step 1	Log into the CMS Enterprise Portal Locate the **Welcome <First Name> <Last Name>** drop-down list at the top-right corner of the page and select **My Profile**. 
Step 2	The 'View My Profile' page displays. Locate the "Screen Reader Mode [Off/On]" and "Accessibility Settings" links in the top-left corner. 
Step 3	Click **Screen reader mode Off** to toggle it to **Screen reader mode On**. 
Step 4	Click **Accessibility Settings** to access more options. 

	Action
Step 5	The ‘Accessibility Preferences’ page displays. Make your selections and click **OK**.



Appendix B: Application Help Desk Information

Application *(Help Desk Name)*	Phone	E-mail
Agents and Brokers (FFM - A/B) *(XOSC)*	855-267-1515	cms_feps@cms.hhs.gov
ASETT *(ASETT Help Desk)*	703-951-6810	asett@actionet.com
BCRS *(COB&R Help Desk)*	888-268-6495	cobrhelp@strategichs.com
Bundled Payments EFT *(Bundled Payments Help Desk)*	N/A	BundledPayments@cms.hhs.gov
CERRS *(Cognosante Help Desk)*	703-206-6199	servicedesk@cognosante.com
Cisco WebEx SaaS *(WebEx Support)*	410-786-3090 *(Option 1)*	OTS_WebEx@cms.hhs.gov
COB *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
Connexion *(CBIC Help Desk)*	877-577-5331	CBIC.admin@palmettogba.com
CPMS *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov
CSR *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
DBidS/ DMEPOS *(CBIC Help Desk)*	877-577-5331	CBIC.admin@palmettogba.com
ECRS *(EDI Help Desk)*	646-458-6740	ECRSHelp@EHMedicare.com
ELMO *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
EPPE *(EPPE Help Desk)*	844-377-3382	eppe@cms.hhs.gov
e-RPT *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
ESD *(ESD Application Support)*	TBD	TBD
FCSO aka The Spot *(FCSO Help Desk)*	855-416-4199	FCSOSpotHelp@FCSO.com
FFSDCS *(ASP Help Desk)*	844-876-0765	aspHelpDesk@dcca.com CLFShelpdesk@dcca.com

Application *(Help Desk Name)*	**Phone**	**E-mail**
Gentran *(Gentran Support)*	N/A	Gentran-support@cms.hhs.gov
HDT *(MCARE/HDT Help Desk)*	866-324-7315	mcare@cms.hhs.gov
HIOS *(XOSC)*	855-267-1515	cms_feps@cms.hhs.gov
IC (Innovation Center) (IBOSC and IC Help Desks)	844-711-CMMI *(Option #1)* 844-280-5628 800-381-4724	cjrsupport@cms.hhs.gov HHVBPquestions@cms.hhs.gov cpcplus@telligen.com
ISV *(ISV Help Desk)*	N/A	ISV-Support@cms.hhs.gov
MACPro *(MACPro Help Desk)*	301-547-4688	MACPro_HelpDesk@cms.hhs.gov
MARx *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
MCU *(XOSC)*	855-267-1515	CMS_feps@cms.hhs.gov
MDR *(MAPD Help Desk)*	800-927-8069	mapdhelp@cms.hhs.gov
MED *(EUS Help Desk)*	866-484-8049	eussupport@cgi.com
MLMS *(MLMS Help Desk)*	N/A	MLMSHelp_Desk@cms.hhs.gov
MyCGS *(MyCGS Help Desk)*	866-270-4909	cgs.dme.mac.email.inquiries@cgsadmin.com
Novitas *(Novitas Help Desk)*	855-880-8424	WebsiteEDI@novitas-solutions.com
Open Payments *(Open Payments Help Desk)*	855-326-8366	OpenPayments@cms.hhs.gov
Physicians Value aka PV *(PV Help Desk)*	888-734-6433	pvHelp_Desk@cms.hhs.gov
PMDA *(PMDA Help Desk)*	443-775-3226	pmda1115_cvp_help@cvpcorp.com
PQRS *(QualityNet Help Desk)*	866-288-8912	qnet-hd-support-queue@hcqis.org

Application *(Help Desk Name)*	Phone	E-mail
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 C: Acronyms

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

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

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

Table 3: Acronyms