



Centers for Medicare & Medicaid Services

CMS.gov Quick Reference Guide - Multi-Factor Authentication (MFA) Optional

April 6, 2016
Version 0.2 Final

Table of Contents

1.	Introduction	2
2.	Step-by-Step Instructions to Request a Role	3
3.	Multi-Factor Authentication (MFA) Optional Function	8
4.	Step-by-Step Instructions to Login with MFA	14
5.	Remove MFA Registration	18
6.	Step-by-Step Instructions for Existing Users Adding MFA	20

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

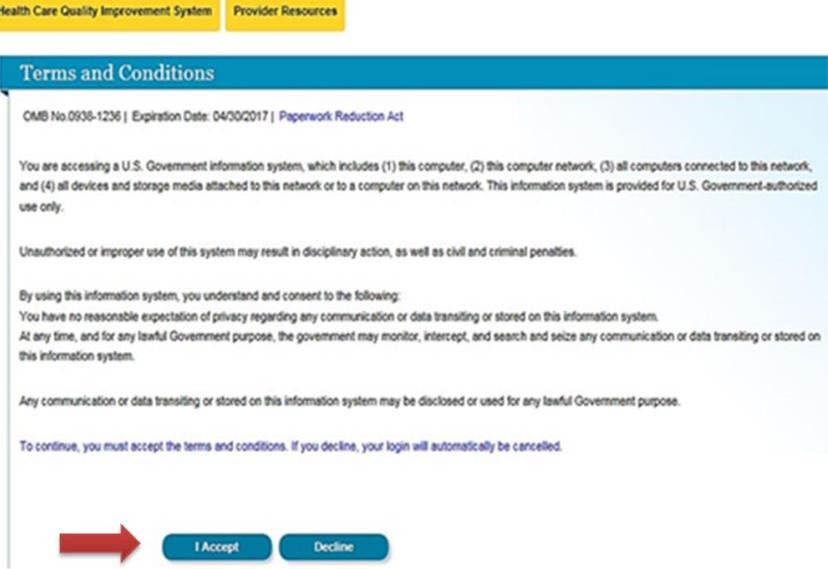
1. Introduction

This guide provides step-by-step instructions on how users with an active CMS.gov Enterprise Portal account complete a role request with an option to log in with Multi-Factor Authentication (MFA) to gain access to CMS applications. Users who are Identity Proofed to a Level of Assurance (LOA) 3 are required to log in with MFA at all times and do not have the option to skip adding an MFA device.

Note: Do not use this guide if you do not have a role in <**Your Application Name**>. If you want to request a role in <**Your Application Name**>, refer to the 'EIDM Quick Reference Guide for New Users Completing RIDP and MFA'. If you do not have a CMS.gov Enterprise Portal account and want to register for one, visit <https://portal.cms.gov>.

2. Step-by-Step Instructions to Request a Role

Please follow each step listed below unless otherwise noted.

Steps	Screenshots
<p>1. Go to https://portal.cms.gov/ and select Login to CMS Secure Portal on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following internet browsers:</i></p> <ul style="list-style-type: none"> • Internet Explorer 8, 9, 10, and 11 • Mozilla-Firefox • Chrome • Safari 	
<p>2. Read the Terms and Conditions and select I Accept to continue.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

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

The screenshot shows the CMS.gov Enterprise Portal login page. At the top, there is a navigation bar with links for Home, About CMS, Newsroom, Archive, Help & FAQs, Email, and Print. Below the navigation bar, there are two yellow buttons: "Health Care Quality Improvement System" and "Provider Resources". The main heading is "Welcome to CMS Enterprise Portal". The login form contains a "User ID" input field with a red arrow pointing to it from the right. Below the input field are two buttons: "Next" and "Cancel", with a red arrow pointing to the "Next" button from the left. At the bottom of the form, there are links for "Forgot User ID?" and "Need an account? Click the link - New user registration".

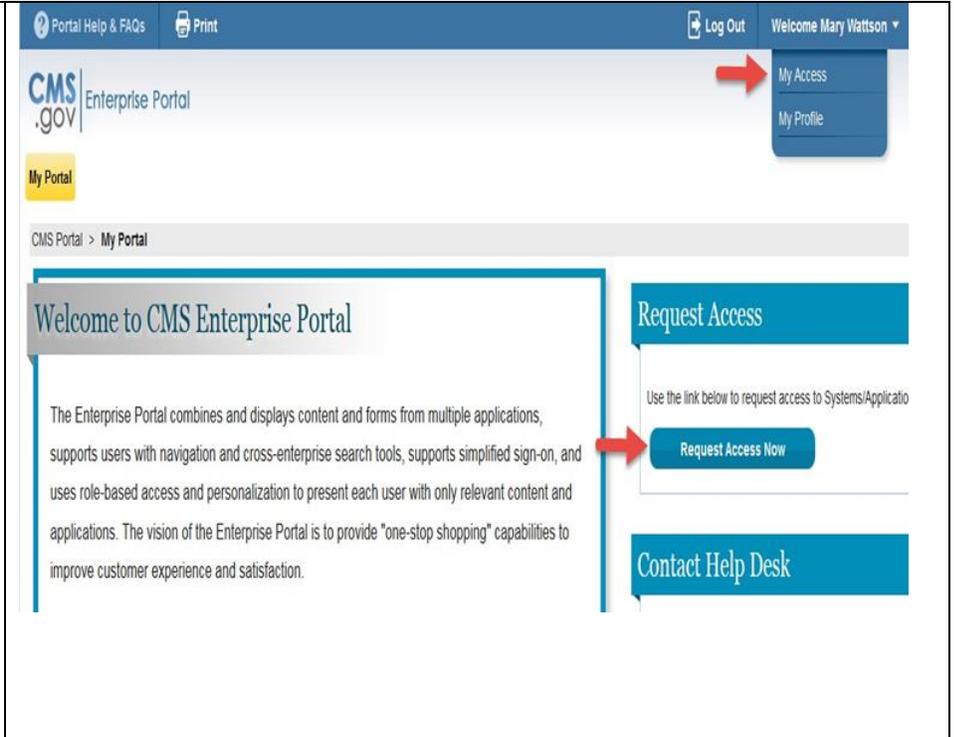
4. Enter your *Password* and select *Log In*.

The screenshot shows the CMS.gov Enterprise Portal login page. At the top, there is a navigation bar with links for Home, About CMS, Newsroom, Archive, Help & FAQs, Email, and Print. Below the navigation bar, there are two yellow buttons: "Health Care Quality Improvement System" and "Provider Resources". The main heading is "Welcome to CMS Enterprise Portal". The login form contains a "Password" input field with a red arrow pointing to it from the right. Below the input field are two buttons: "Log In" and "Cancel", with a red arrow pointing to the "Log In" button from the left. At the bottom of the form, there is a link for "Forgot Password?".

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

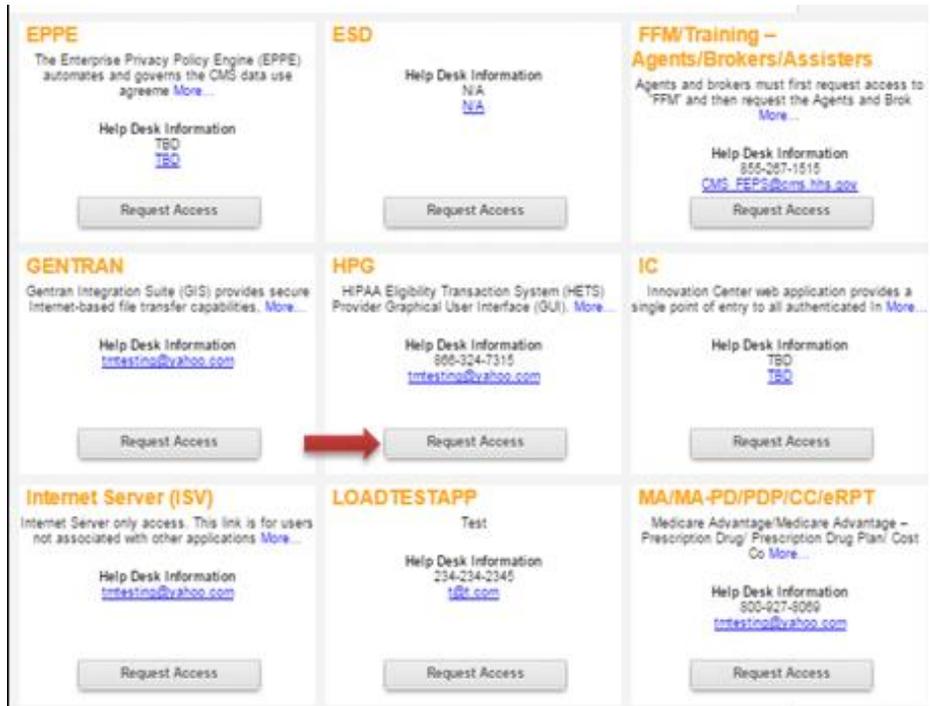
5. Select **Request Access Now** under **Request Access** to begin the process of requesting a new user role.

*Note: You may also select your username at the top right corner and then select **My Access** from the drop-down menu to begin the process of requesting a new user role.*



If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

6. Look for your application in the Access Catalog and select **Request Access**.



7. Select the application role that you want to request from the drop-down menu of the **Select a Role** field.

Select **Next** to begin the **Remote Identify Proofing (RIDP)** process.

Note: The Next button will only be visible after selecting a role and providing the required information.



If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

8. Select *Next* to proceed.

Note: Please reference the EIDM Quick Reference Guide 'EIDM QRG – New Users Completing RIDP and MFA' for detailed steps for the identity verification process.

Request New Application Access

Identity Verification

To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind.

1. Ensure that you have entered your legal name, current home address, primary phone number, date of birth and E-mail address correctly. We will only collect personal information to verify your identity with Experian, an external Identity Verification provider.
2. Identity Verification involves Experian using information from your credit report to help confirm your identity. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and you do not incur any charges related to them.
3. You may need to have access to your personal and credit report information, as the Experian application will pose questions to you, based on data in their files. For additional information, please see the Experian Consumer Assistance website -<http://www.experian.com/help/>

If you elect to proceed now, you will be prompted with a Terms and Conditions statement that explains how your Personal Identifiable Information (PII) is used to confirm your identity. To continue this process, select 'Next'.



9. **Remote Identity Proofing** is now complete. Select *Next* to proceed to optional registration for **Multi-Factor Authentication (MFA)**.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

3. Multi-Factor Authentication (MFA) Optional Function

MFA is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

MFA requires you to provide more than one form of verification in order to prove your identity. MFA registration is required only once when you are requesting a role, but will be verified every time you log into the CMS Enterprise Portal.

During the MFA registration process, the CMS.gov Enterprise Portal requires registration of a phone, computer, or email to add an additional level of security to a user’s account.

You may select from the following options to complete the registration process:

- **Smart Phone:** Download Verification and Identity Protection (VIP) access software on your smart phone/tablet. You must enter the alphanumeric credential ID that is generated by the VIP access client. You will then enter the Security Code generated by the VIP client.
- **Computer:** Download VIP access software on your computer. You must enter the alphanumeric credential ID generated by the VIP access client. You will then enter the Security Code generated by the VIP client.
- **E-mail:** Select the e-mail option to receive an e-mail containing a Security Code required at login. You must provide a valid, accessible e-mail address.
- **Short Message Service (SMS):** Use the SMS option to have your Security Code texted to your phone. You must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR):** Select the IVR option to receive a voice message containing your Security Code. You must provide a valid phone number and (optional) phone extension.

MFA Optional – Add MFA

During a role request, a user who is Identity Proofed to LOA 2, has the option to add MFA to their profile or skip this process. This section will go through the steps to complete the process of adding MFA to your user profile.

Please follow steps 10 – 13 to continue role request with registering an MFA Device.

Steps	Screenshots
-------	-------------

10. Select **Add MFA** to begin device setup for the **Multi-Factor Authentication** login.

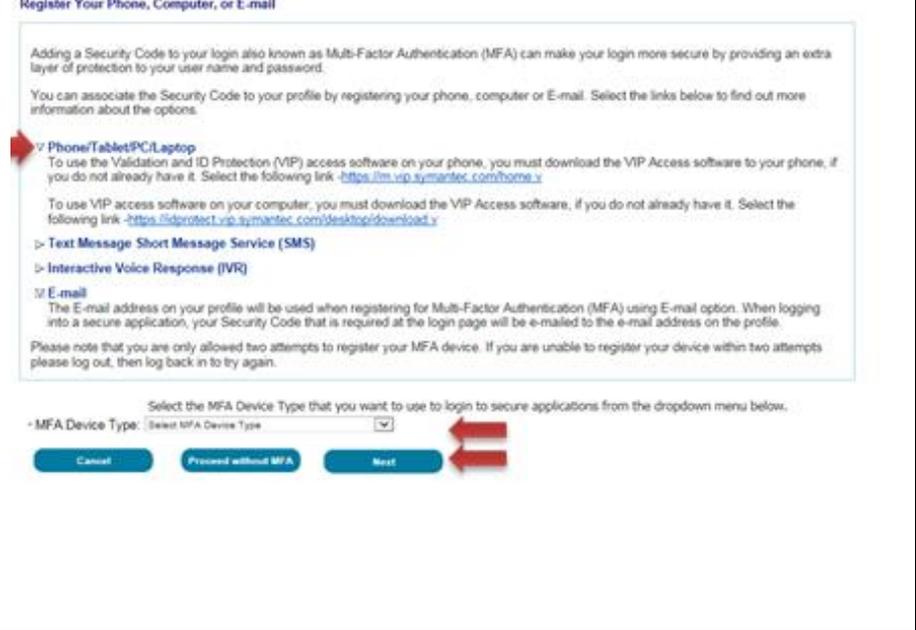


11. Select an MFA device from the **MFA Device Type** drop-down.

Note: You can select the arrows on the left of each MFA Device Type for additional information.

*If you wish to continue without MFA, select **Proceed without MFA**. You will be directed to the next step of the role request (see step 14).*

Cancel: Selecting this will end the role request.



If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

11(a). If selecting **Phone/Tablet/PC/Laptop** as the **MFA Device Type**, enter the alphanumeric code that displays under the field labeled **Credential ID** (on the VIP Access software) in the **Credential ID** field. Enter a brief description (example: *Laptop*) in the field labeled **MFA Device Description**. Then select **Next**.

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 for logging into your application.

Select the MFA Device Type that you want to use for logging into your application.

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

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

Credential ID:

MFA Device Description:

Cancel Proceed without MFA Next



11(b). If selecting **Text Message – Short Message Service (SMS)** as the **MFA Device Type**, enter the **Phone Number** that will be used to obtain the Security Code. Enter a brief description (example: *Text*) in the field labeled **MFA Device Description** and select **Next**.

Select the MFA Device Type that you want to use for logging into your application.

Select the credential type that you want to use for logging into your application.

MFA Device Type: **Text Message-Short Message service(SMS)**

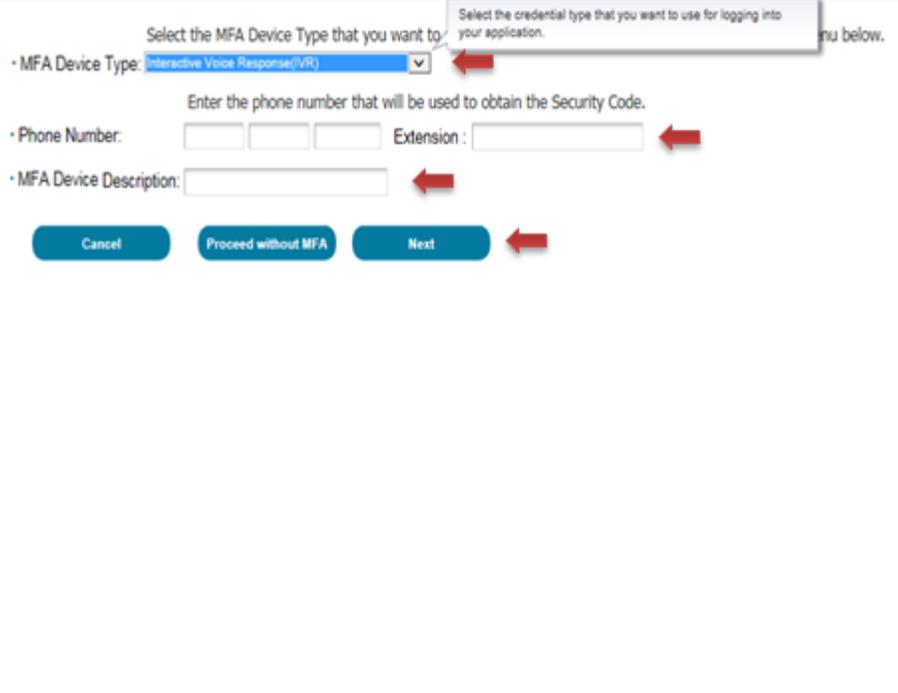
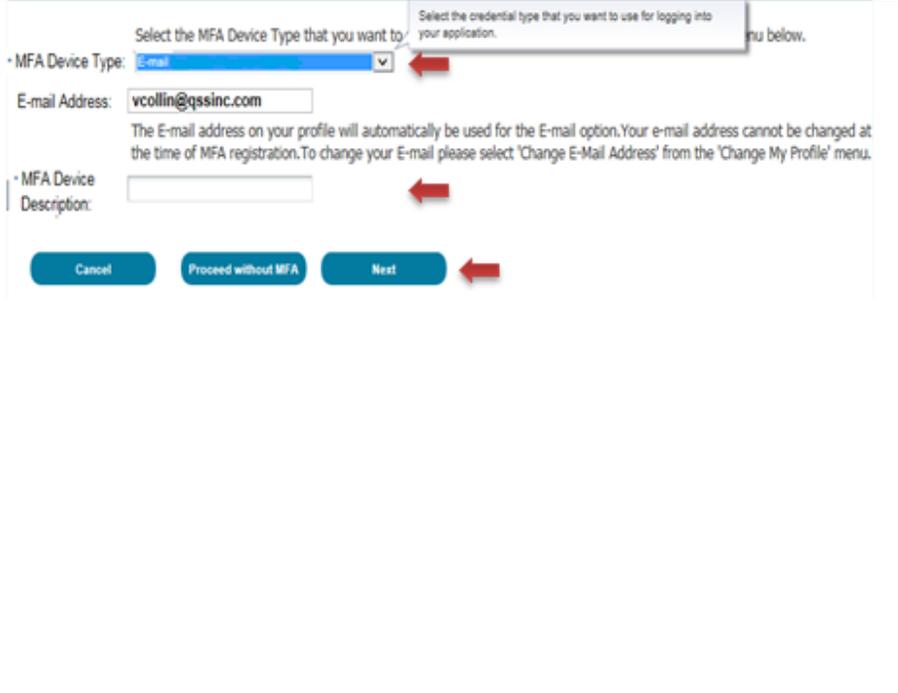
Enter the phone number that will be used to obtain the Security Code.

Phone Number:

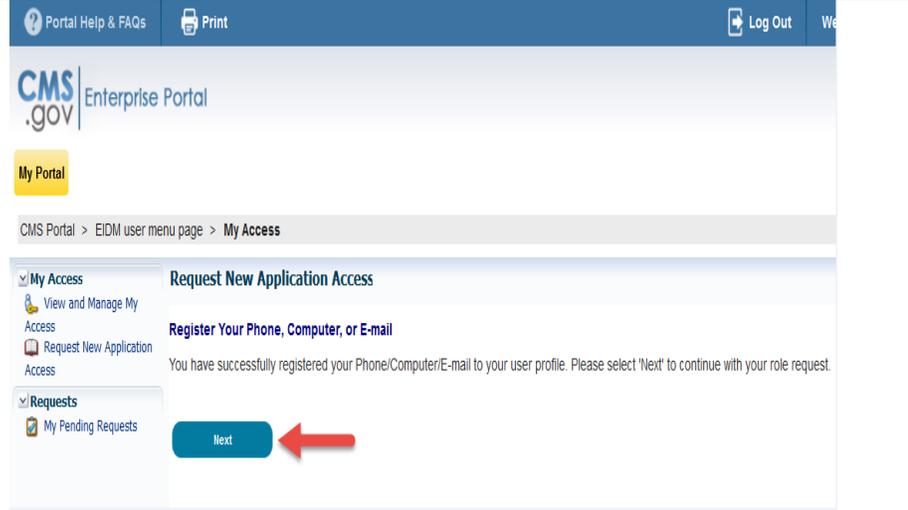
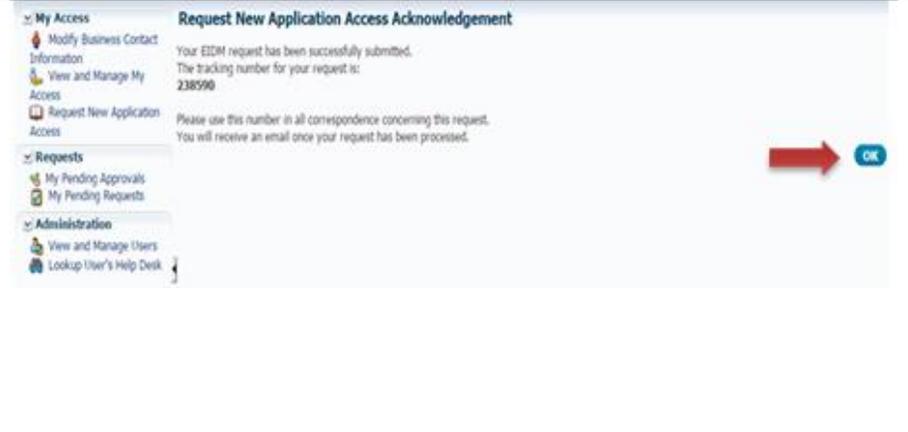
MFA Device Description:

Cancel Proceed without MFA Next

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

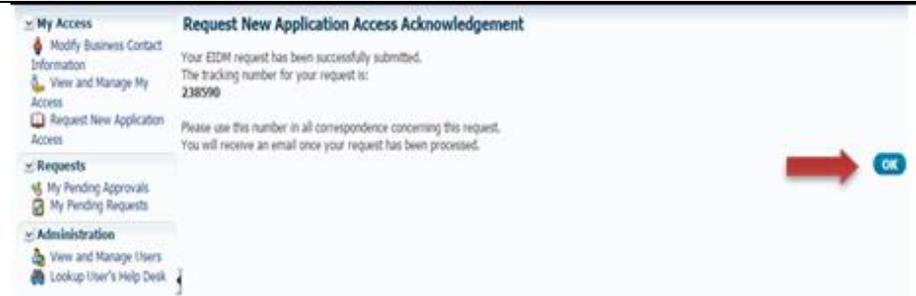
<p>11(c). If selecting Voice Message – Interactive Voice Response (IVR) as the MFA Device Type, enter the Phone Number and corresponding Extension that will be used to obtain the Security Code. Enter a brief description (example: <i>IVR</i>) in the field labeled MFA Device Description and select Next.</p> <p>Note: <i>Extension</i> is an optional field. You may choose to provide a 10-digit phone number or a phone number with an extension.</p>	 <p>The screenshot shows the MFA registration interface for IVR. At the top, there are two instructional boxes: 'Select the MFA Device Type that you want to use for logging into your application.' and 'Select the credential type that you want to use for logging into your application.' Below these, the 'MFA Device Type' dropdown menu is set to 'Interactive Voice Response (IVR)'. The 'Phone Number' field is empty, and the 'Extension' field is empty. The 'MFA Device Description' field is empty. At the bottom, there are three buttons: 'Cancel', 'Proceed without MFA', and 'Next'. The 'Next' button is highlighted with a red arrow.</p>
<p>11(d). If selecting E-mail as the MFA Device Type, the E-mail address on your profile will be automatically used to obtain the Security Code. Enter a brief description (example: <i>E-mail</i>) in the field labeled MFA Device Description and select Next.</p> <p>Note: <i>The E-mail address cannot be changed at the time of MFA device registration. It can only be changed using the 'Change E-Mail Address' option from the 'Change My Profile' menu.</i></p>	 <p>The screenshot shows the MFA registration interface for E-mail. At the top, there are two instructional boxes: 'Select the MFA Device Type that you want to use for logging into your application.' and 'Select the credential type that you want to use for logging into your application.' Below these, the 'MFA Device Type' dropdown menu is set to 'E-mail'. The 'E-mail Address' field is populated with 'vcollin@qssinc.com'. Below the email field, there is a note: 'The E-mail address on your profile will automatically be used for the E-mail option. Your e-mail address cannot be changed at the time of MFA registration. To change your E-mail please select 'Change E-Mail Address' from the 'Change My Profile' menu.' The 'MFA Device Description' field is empty. At the bottom, there are three buttons: 'Cancel', 'Proceed without MFA', and 'Next'. The 'Next' button is highlighted with a red arrow.</p>

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

<p>12. Your registration for Multi-Factor Authentication is now complete. Select Next to complete the role request process.</p>	
<p>13. If the role requires approval, a message will display with a tracking number for your request. An email will be sent once your request has been approved or rejected. Select OK to continue.</p>	
<p>MFA Optional – Skip MFA</p> <p>The next section will go through the steps to skip registering a device for MFA via “Skip MFA”.</p> <p>Please follow steps 14 - 15 to continue the role request process without registering an MFA Device.</p>	
<p>14. Select Skip MFA to begin device setup for the Multi-Factor Authentication login.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

15. If the role requires approval, a message will display with a tracking number for your request. An email will be sent once your request has been approved or rejected. Select **OK** to continue.



If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

4. Step-by-Step Instructions to Login with MFA

The login experience will be different once an MFA Device has been registered to your user profile. Please follow steps 16 - 19 to log in with an MFA Device.

Steps	Screenshots
<p>16. Go to https://portal.cms.gov/ and select Login to CMS Secure Portal on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following internet browsers:</i></p> <ul style="list-style-type: none"> • <i>Internet Explorer 8, 9, 10, and 11</i> • <i>Mozilla-Firefox</i> • <i>Chrome</i> • <i>Safari</i> 	 <p>The screenshot shows the CMS.gov Enterprise Portal homepage. At the top, there is a navigation bar with links for Home, About CMS, Newsroom, Archive, Help & FAQs, Email, and Print. Below this is a search bar and a 'Search CMS.gov' button. The main content area features a large banner with the text 'Welcome to CMS Enterprise Portal' and a description of the portal as a gateway for Medicare Advantage, Prescription Drug, and other CMS programs. On the right side of the banner, there is a 'CMS Secure Portal' section with a 'Login to CMS Secure Portal' button. A red arrow points to this button. Below the button are links for 'Forgot User ID?', 'Forgot Password?', and 'New User Registration'. At the bottom of the page, there is a horizontal menu with various program links such as Medicare Shared Savings Program, Physician Value, ASP, Open Payments, QMAT, CPC, Innovation Center, MLMS, INCU, PECOS, Quality Reporting, and CBIC.</p>

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

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

Health Care Quality Improvement System | Provider Resources

Terms and Conditions

OMB No.0538-1236 | Expiration Date: 04/30/2017 | Paperwork Reduction Act

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.
At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.

 **I Accept** Decline

18. Enter your ***User ID*** and select ***Next***.

Home | About CMS | Newsroom | Archive | Help & FAQs | Email | Print

CMS.gov | Enterprise Portal

Centers for Medicare & Medicaid Services

Health Care Quality Improvement System | Provider Resources

Welcome to CMS Enterprise Portal

User ID 

 **Next** **Cancel**

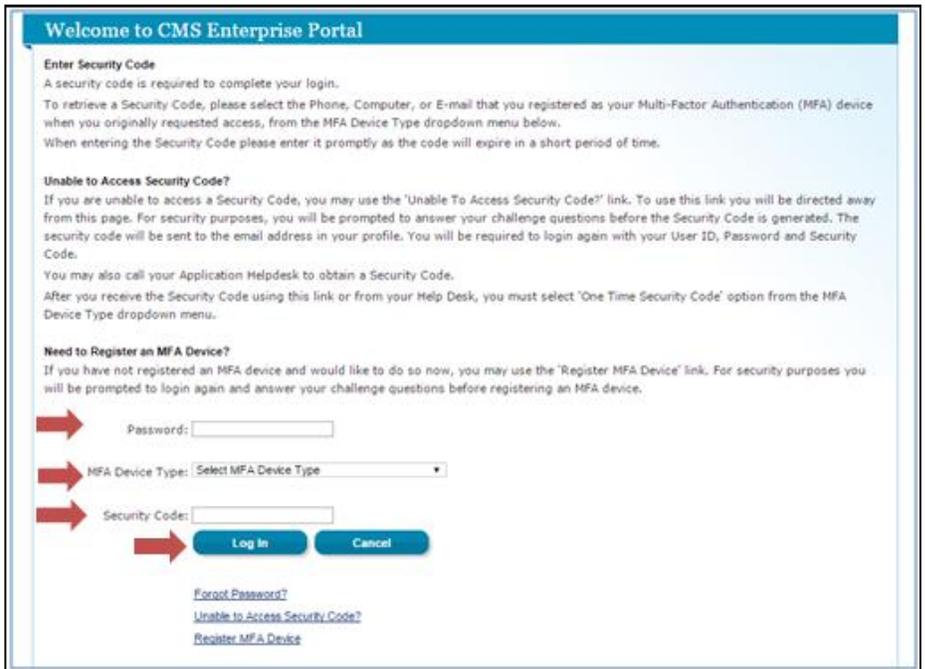
[Forgot User ID?](#)
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

19. Enter your Password, select an MFA device from the **MFA Device Type** drop-down, and select **Log In**.

Note: The Security Code for E-mail and One-Time Security Code will expire in 30 minutes. The Security Code for the other MFA device types will expire in 10 minutes. If you are unable to enter the code within the period, you will need to request a new Security Code.

If you do not have access to your registered MFA device, please refer to the EIDM Quick Reference Guide 'EIDM QRG – User Login', for step-by-step instructions on how to register an MFA Device.



19(a). If you selected **Phone/Tablet/PC/Laptop** as the **MFA Device Type**, enter the Security Code that displays under the field labeled Security Code (on the VIP Access software) in the **Security Code** field. Select **Log In**.



If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

19(b). If you selected **Text Message – Short Message Service (SMS)** or **Interactive Voice Response (IVR)** or **E-mail** as the **MFA Device Type**, select **Send** to receive the Security Code on the selected MFA device type. Enter the Security Code in the **Security Code** field and select **Log In**.

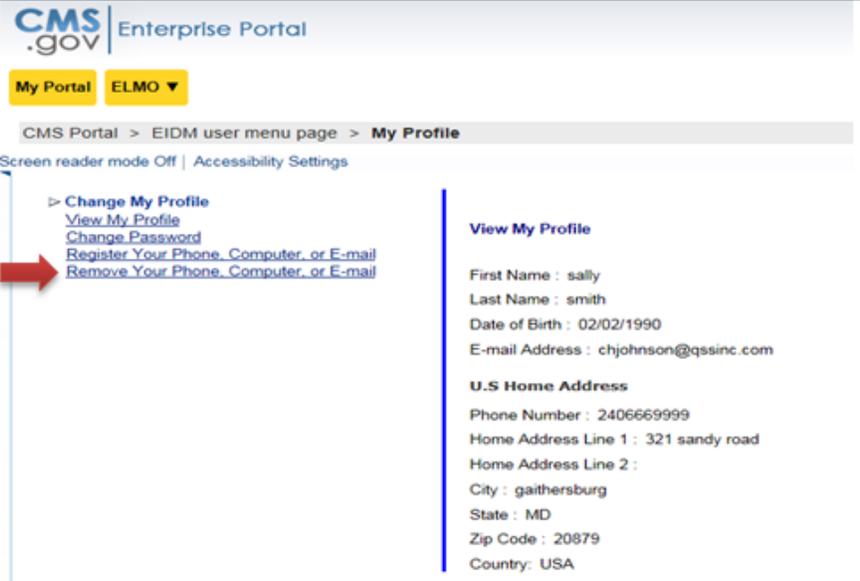
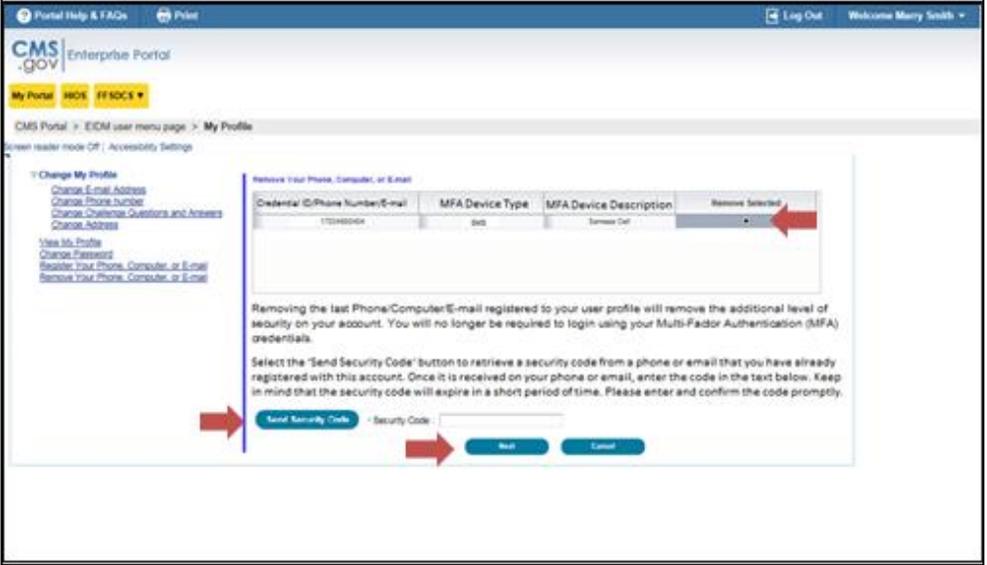
19(c). If you selected **One-Time Security Code** as the **MFA Device Type**, enter the Security Code that was sent to your registered E-mail address via the ‘Unable to Access Security Code?’ link or provided by the Helpdesk, in the **Security Code** field. Select **Log In**.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

5. Remove MFA Registration

Users at LOA 2 can remove the option of MFA at any time by removing all registered MFA devices from their profile. By removing the last MFA device, the user will no longer be required to log in with MFA.

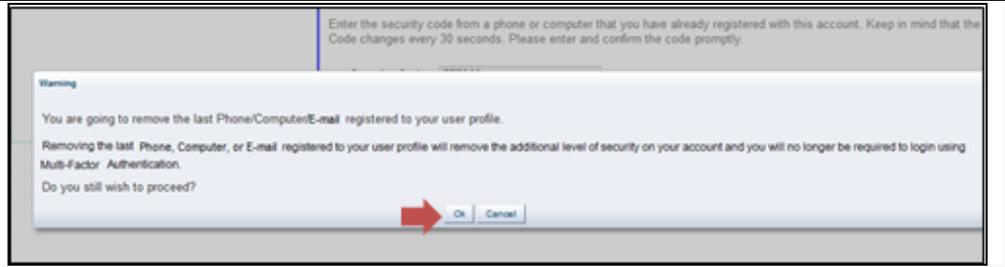
Please follow steps 20 - 23 to Remove MFA Registration.

Steps	Screenshots
<p>20. Select the Remove Your Phone, Computer, or E-mail link to remove a registered MFA device from your profile.</p>	 <p>The screenshot shows the 'My Profile' page with a navigation menu on the left. A red arrow points to the link 'Remove Your Phone, Computer, or E-mail'.</p>
<p>21. Select the registered device you want to remove, select Send Security Code, enter the security code received on the selected MFA device type, and select Next to proceed.</p> <p><i>Note: Selecting Cancel will end the device removal process.</i></p>	 <p>The screenshot shows a confirmation dialog with a table of MFA devices. A red arrow points to the 'Remove Selected' button. Below the table, there is a 'Send Security Code' button and a 'Security Code' input field. Another red arrow points to the 'Send Security Code' button.</p>

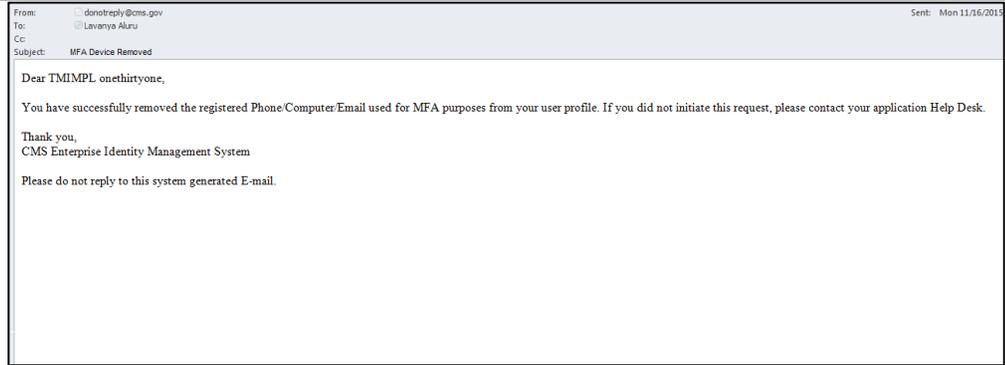
If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

22. Select **OK** to remove the MFA device.

Note: If you are Identity Proofed to LOA 3, you will be required to have at least one device registered to your profile.



23. Once the MFA Device is removed from your user profile, a confirmation email will be sent to the registered email address in your user profile.

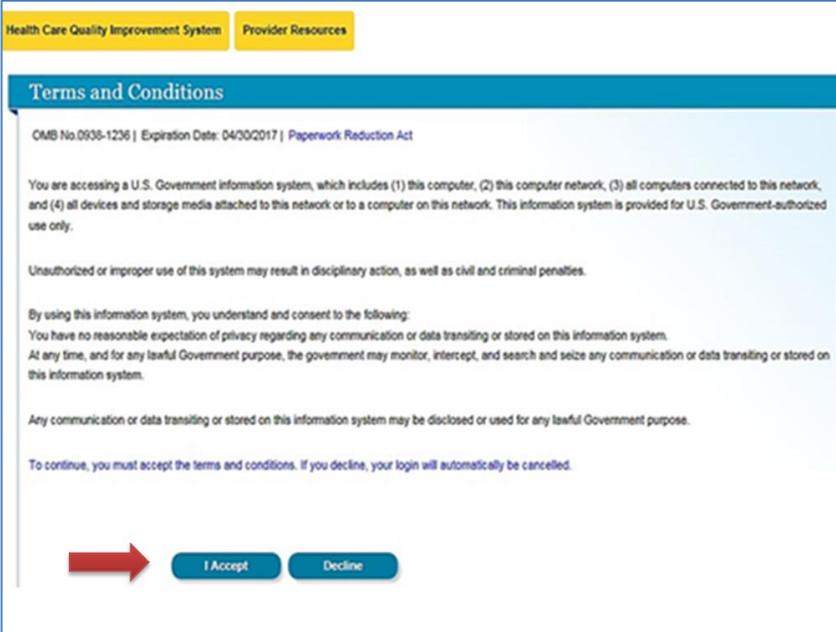


If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

6. Step-by-Step Instructions for Existing Users Adding MFA

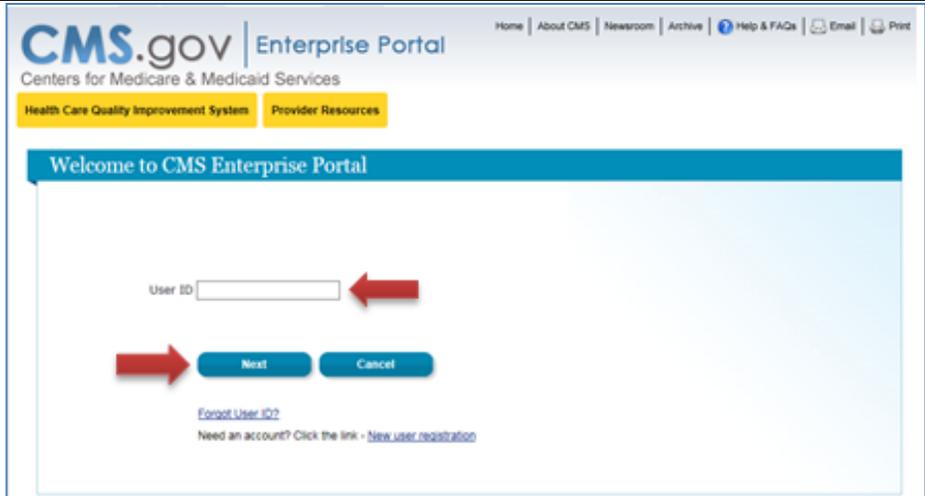
Users with roles configured for optional MFA can add an additional level of security to their login process by registering an MFA device to their profile at any time. By adding an MFA device, the user will be required to log in with an MFA Security Code.

Please follow steps 1 - 8 to Add MFA Registration.

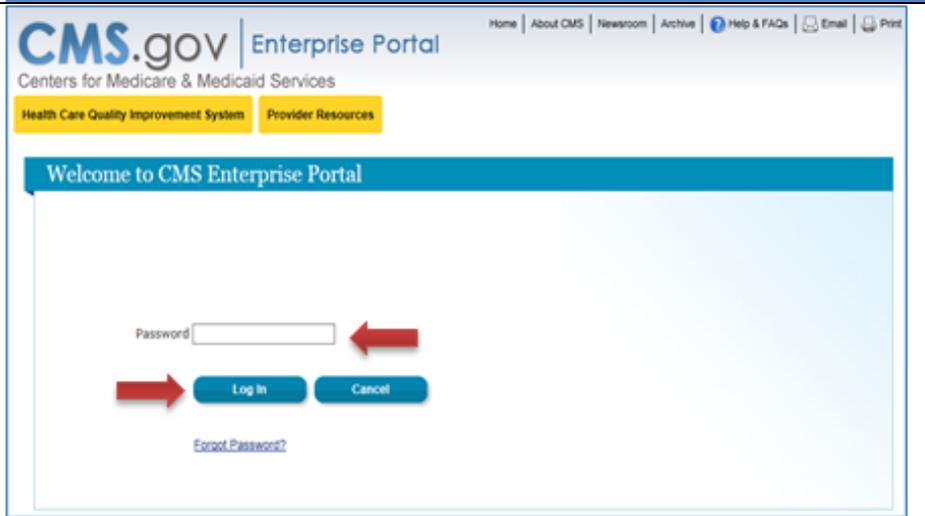
Steps	Screenshots
<p>1. Go to https://portal.cms.gov/ and select Login to CMS Secure Portal on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following internet browsers:</i></p> <ul style="list-style-type: none"> • Internet Explorer 8, 9, 10, and 11 • Mozilla-Firefox • Chrome • Safari 	
<p>2. Read the Terms and Conditions and select I Accept to continue.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

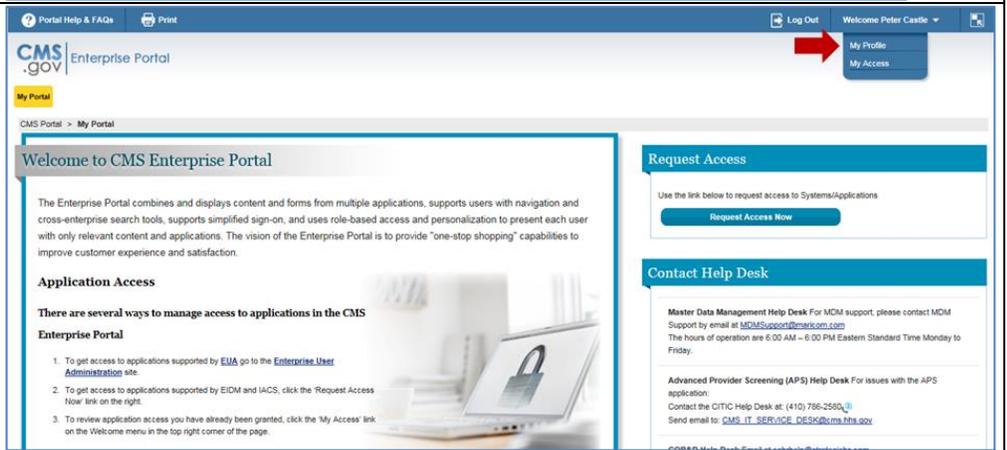
3. Enter your *User ID* and select *Next*.



4. Enter your *Password* and select *Log In*.



5. Select your username at the top right corner and then select *My Profile* from the drop-down menu to begin the process of registering for MFA.



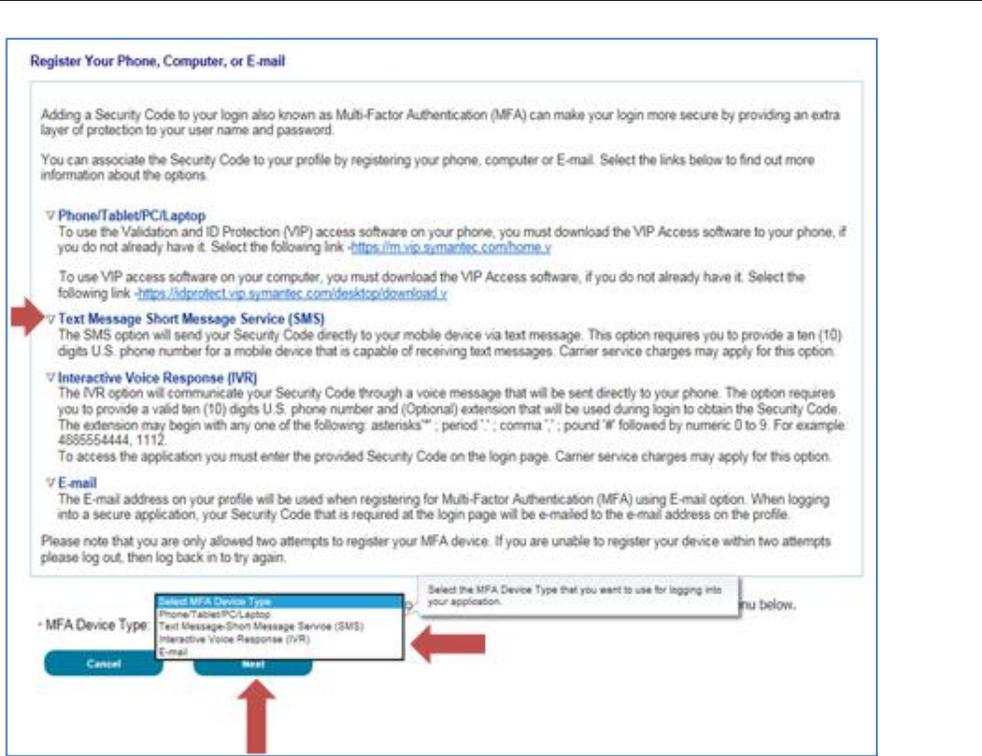
If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

6. Select the **Register Your Phone, Computer, or E-mail** link to register an MFA device to your profile.



7. Select an MFA device from the **MFA Device Type** drop-down and select **Next**.

Note: You can select the arrows on the left of each MFA Device Type for additional information.



7. (a) If selecting **Phone/Tablet/PC/Laptop** as the **MFA Device Type**, enter the alphanumeric code that displays under the field labeled Credential ID (on the VIP Access software) in the **Credential ID** field. Enter a brief description (example: *Laptop*) in the field labeled **MFA Device Description**.

MFA Option (a) Screenshots

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

Then select *Next*.

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**
To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>
To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

▼ **Text Message Short Message Service (SMS)**
The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

▼ **Interactive Voice Response (IVR)**
The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will 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: 489554444, 1112.
To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

▼ **E-mail**
The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

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: ▼

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

• Credential ID:

• MFA Device Description:



If you have questions or need assistance regarding MFA, please contact your Application Help Desk.

OR

7. (b) If selecting **Text Message – Short Message Service (SMS)** as the **MFA Device Type**, enter the **Phone Number** that will be used to obtain the Security Code. Enter a brief description (example: *Text*) in the field labeled **MFA Device Description** and select **Next**.

OR

MFA Option (b) Screenshot

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
To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>
To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

Text Message Short Message Service (SMS)
The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

Interactive Voice Response (IVR)
The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will 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: 488554444, 1112.
To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

E-mail
The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

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: Text Message-Short Message Service (SMS)

Enter the phone number that will be used to obtain the Security Code.

Phone Number: 111 222 3333

MFA Device Description: Text

Cancel Next

OR

7. (c) If selecting **Voice Message – Interactive Voice Response (IVR)** as the **MFA Device Type**, enter the **Phone Number** and corresponding **Extension** that will be used to obtain the Security Code as **Phone Number** and **Extension**. Enter a brief description (example: *IVR*) in the field labeled **MFA Device Description** and select **Next**.

Note: Extension is optional. You may choose to provide a 10-digit phone number or phone number with an extension.

OR

MFA Option (c) Screenshot

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
To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>
To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

Text Message Short Message Service (SMS)
The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

Interactive Voice Response (IVR)
The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will 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: 488554444, 1112.
To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

E-mail
The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

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: Interactive Voice Response (IVR)

Enter the phone number that will be used to obtain the Security Code.

Phone Number: 607 345 2423 **Extension:** 242

MFA Device Description: IVR

Cancel Next

OR

7. (d) If selecting **E-mail** as the **MFA Device Type**, the E-mail address on your profile will be automatically used to obtain the Security Code. Enter a brief description (example: *E-mail*) in the field labeled **MFA Device Description** and select **Next**.

Note: The E-mail address cannot be changed at the time of MFA device registration. It can only be changed using the 'Change E-Mail Address' option from the 'Change My Profile' menu.

OR

MFA Option (d) Screenshot

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**
To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>
To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>
- Text Message Short Message Service (SMS)**
The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.
- Interactive Voice Response (IVR)**
The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks "*", period ".", comma ",", pound "W" followed by numeric 0 to 9. For example: 4885554444, 1112.
To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.
- E-mail**
The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.
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:

E-mail Address:

The E-mail address on your profile will automatically be used for the E-mail option. Your e-mail address cannot be changed at the time of MFA registration. To change your E-mail please select 'Change E-Mail Address' from the 'Change My Profile' menu.

MFA Device Description:

8. Your registration for the MFA is now complete. Select **OK** to be directed to your **My Profile** page.

Note: You will receive an E-mail notification for successfully registering the MFA device type.

CMS.gov Enterprise Portal

My Portal

CMS Portal > EIDM user menu page > **My Profile**

Screen reader mode Off | Accessibility Settings

- Change My Profile**
 - [Change E-mail Address](#)
 - [Change Phone number](#)
 - [Change Challenge Questions and Answers](#)
 - [Change Address](#)
- [View My Profile](#)
- [Change Password](#)
- [Register Your Phone, Computer, or E-mail](#)
- [Remove Your Phone or Computer](#)

Register Your Phone, Computer, or E-mail

You have successfully registered your Phone/Computer/E-mail to your user profile

If you have questions or need assistance regarding MFA, please contact your Application Help Desk.