



Centers for Medicare & Medicaid Services

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

August 2015
Draft Version 0.2

Table of Contents

1.	Introduction _____	2
2.	Step-by-Step Instructions to Register for Multi-Factor Authentication (MFA) in EIDM _____	3
3.	Remove a Registered Multi-Factor Authentication (MFA) Device _____	12
4.	Multi-Factor Authentication (MFA) Completed when Accessing a Protected-URL/Resource.	Error! Bookmark not defined.

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

1. Introduction

This guide provides step-by-step instructions on how users who already have an active CMS.gov Enterprise Portal account and a role in MAPD / MARx can register for EIDM Multi Factor Authentication (MFA), remove a registered MFA device and login with Multi-Factor Authentication when accessing an application resource/URL that is MFA protected.

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

2. Step-by-Step Instructions to Register for Multi-Factor Authentication (MFA) in CMS.gov Enterprise Portal

Please follow each step listed below unless otherwise noted.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

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

Registered CMS.gov Enterprise Portal users with an existing account, who wish to access a CMS MFA protected application, will be directed through the MFA registration process.

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. The user is given five options to select from to complete the registration process. The same steps can be followed to register multiple MFA devices.

Depending on the MFA option you choose to register, you may need access to download and install software on your computer/phone; your phone should be able to receive text messaging (SMS); or you should have a valid email address.

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

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

1. Go to <https://portal.cms.gov/> and Select **Login to CMS Secure Portal** on the **CMS Enterprise Portal**.

Note: The CMS Enterprise Portal supports the following internet browsers:

- Internet Explorer 8
- Internet Explorer 9
- Mozilla-Firefox
- Chrome
- Safari

Enable JavaScript and adjust any zoom features to ensure you are not seeing the screen in too wide of a view.



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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

2. Read **Terms and Conditions** and select ***I Accept*** to continue.

Health Care Quality Improvement System

Provider Resources

Terms and Conditions

OMB No.0938-1236 | 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

3. Enter the following information and select ***Log In***:
 - EIDM User ID
 - EIDM Password

CMS.gov | Enterprise Portal
Centers for Medicare & Medicaid Services

[Home](#) | [About CMS](#) | [Newsroom](#) | [Archive](#) | [?](#)

Health Care Quality Improvement System

Provider Resources

Welcome to CMS Enterprise Portal

User ID

Password



Log In

Cancel

[Forgot Password?](#)

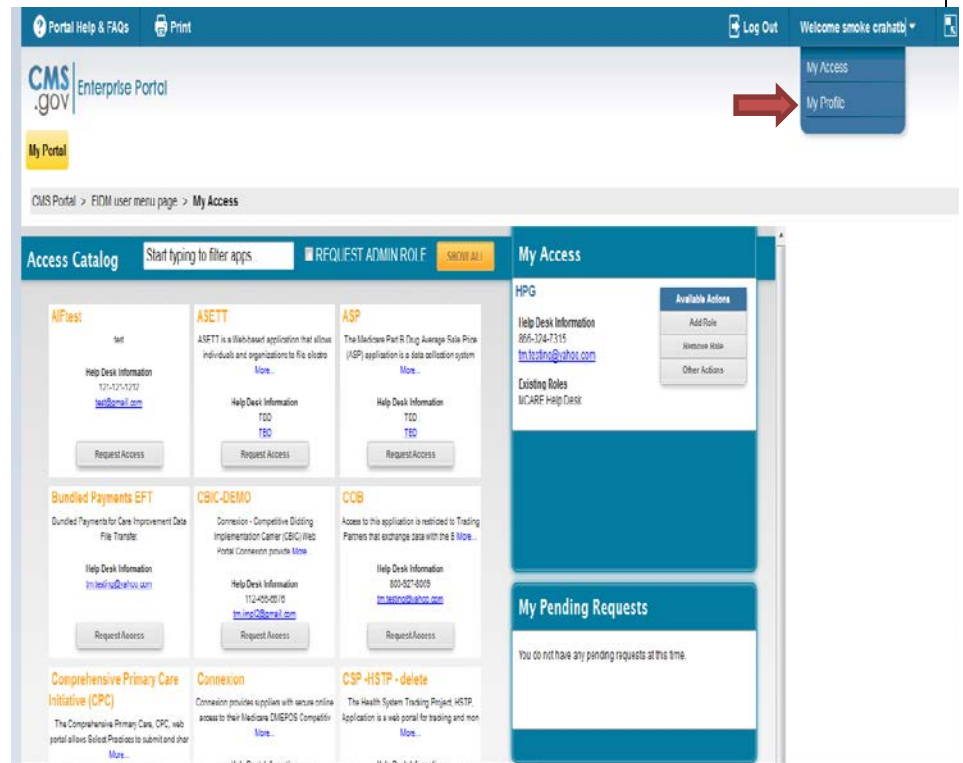
[Forgot User ID?](#)

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

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

4. Select your username and then select **My Profile** from the drop-down menu to go to your profile.



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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

5. Select **Register Your Phone, Computer, or Email** from the navigation links on the left to begin the process of adding MFA to your account.

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](#)

View My Profile

First Name : user
Last Name : change
Date of Birth : 12/12/1964
E-mail Address : rkumbum@qssinc.co

U.S Home Address

Phone Number :
Home Address Line 1 : 6503 Woodlaw
Home Address Line 2 : apt 7888
City : Baltimore
State : MD
Zip Code : 21222
Country: USA

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

7. Read the **Register Your Phone, Computer, or E-mail** notification and then select an option from the **Credential Type** drop-down menu.

Note: *Regardless of the mechanism you choose, you will have 30 seconds to retrieve and enter the Security Code. If you are unable to enter the code within 30 seconds, then the code will expire and you need to request a new Security Code.*

Request New Application Access

Register Your Phone, Computer, or E-mail

You have selected to register another phone, computer or e-mail with your user profile. Select one of the options below to make your account more secure.

If you intend to use 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>

If you intend 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 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. This option requires you to provide a valid phone number. The number that you supplied will be called whenever you attempt to access secure application, and you will be provided with a security code. 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 One Time Password (OTP): The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail OTP option. When logging into a secure application, your One Time Password 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 credential type that you want to use for logging into your application.

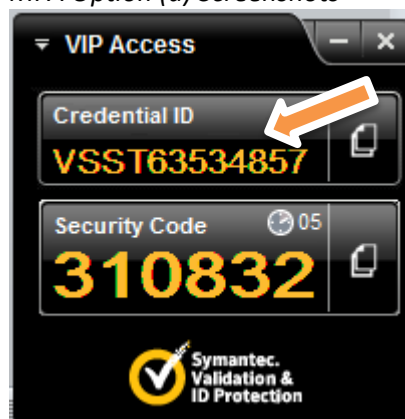
Select the credential type that you want to use

* Credential Type :

- Select Credential type
- Phone/Tablet/PC/Laptop
- E-mail - One Time Password (OTP)
- Text Message - Short Message service (SMS)
- Voice Message - Interactive Voice Response (IVR)

8. (a) If selecting **Phone/Tablet/PC/Laptop** as **Credential Type**, enter the alphanumeric code that displays under the field label **Credential ID** in the **Credential ID** field. Enter brief description in the field labeled **Credential Description**.
OR
(b) If selecting **E-mail – One Time Password (OTP)** as **Credential Type**, the email associated with your CMS.gov Enterprise Portal account should be entered in the field labeled **E-mail Address** to obtain the security

MFA Option (a) Screenshots



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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

code. Enter '**E-mail**' as the **Credential Description**.
OR
(C) If selecting **Text Message – Short Message Service (SMS)** as **Credential Type**, enter the **Phone Number** that will be used to obtain the security code as **Phone Number** and '**Text**' as the **Credential Description**.

OR
(D) If selecting **Voice Message – Interactive Voice Response (IVR)** as **Credential Type**, enter the **Phone Number** that will be used to obtain the security code as **Phone Number** and '**IVR**' as **Credential Description**.

Select **Next** to continue.

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 selected to register another phone, computer, or e-mail with your user profile. Select one of the options below to make your account more secure.

If you intend to use 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>

If you intend 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 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. This option requires you to provide a valid phone number. The number that you supplied will be called whenever you attempt to access secure application, and you will be provided with a security code. 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 One Time Password (OTP). The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail OTP option. When logging into a secure application, your One Time Password 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 credential type that you want to use to login to secure applications from the dropdown menu below.

• Credential Type : Phone/Tables/PC/Laptop

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

• Credential ID : VSST63534857

• Credential Description : VIC Laptop

Cancel Next

OR
MFA Option (b) Screenshots

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

Register Your Phone, Computer, or E-mail

You have selected to register another phone, computer or e-mail with your user profile. Select one of the options below to make your account more secure.

If you intend to use 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>

If you intend 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 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. This option requires you to provide a valid phone number. The number that you supplied will be called whenever you attempt to access secure application, and you will be provided with a security code. 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 One Time Password (OTP): The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail OTP option. When logging into a secure application, your One Time Password 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 credential type that you want to use below.

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

* Credential Type :

E-mail Address:

The E-mail address on your profile will automatically be used for the OTP 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.

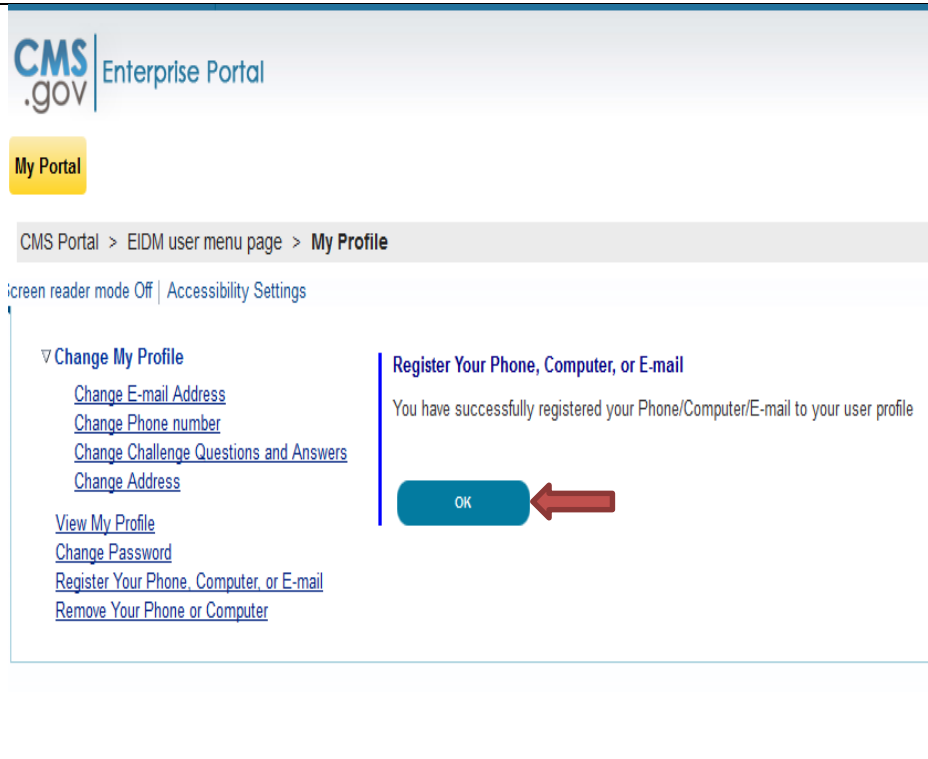
* Credential Description :

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

9. Your registration for the **Multi Factor Authentication** is now complete. Select **OK** to be directed to your profile page.


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



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

3. Remove a Registered Multi-Factor Authentication (MFA) Device

To remove a registered Phone or Computer, 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>Note: The CMS Enterprise Portal supports the following internet browsers:</p> <ul style="list-style-type: none">• Internet Explorer 8• Internet Explorer 9• Mozilla-Firefox• Chrome• Safari <p>Enable JavaScript and adjust any zoom features to ensure you are not seeing the screen in too wide of a view.</p>	

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

2. Read **Terms and Conditions** and select ***I Accept*** to continue.

Health Care Quality Improvement System

Provider Resources

Terms and Conditions

OMB No.0938-1236 | 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

3. Enter the following information and select ***Log In***:
 - EIDM User ID
 - EIDM Password

CMS.gov | Enterprise Portal
Centers for Medicare & Medicaid Services

[Home](#) | [About CMS](#) | [Newsroom](#) | [Archive](#) | [?](#)

Health Care Quality Improvement System

Provider Resources

Welcome to CMS Enterprise Portal

User ID

Password



Log In

Cancel

[Forgot Password?](#)

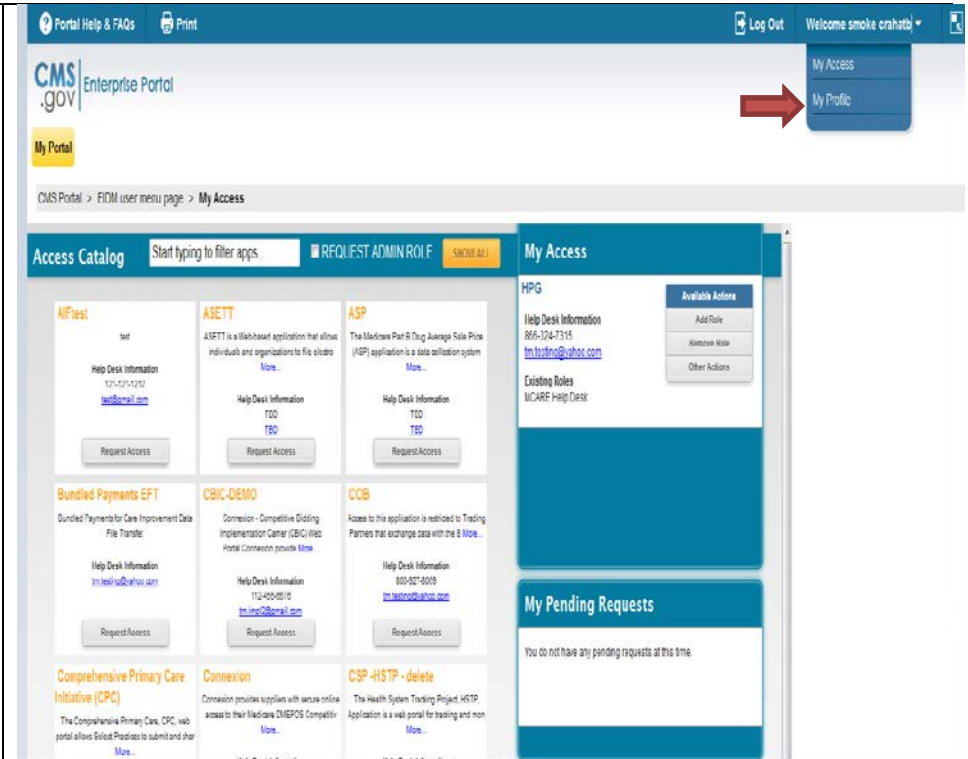
[Forgot User ID?](#)

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

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

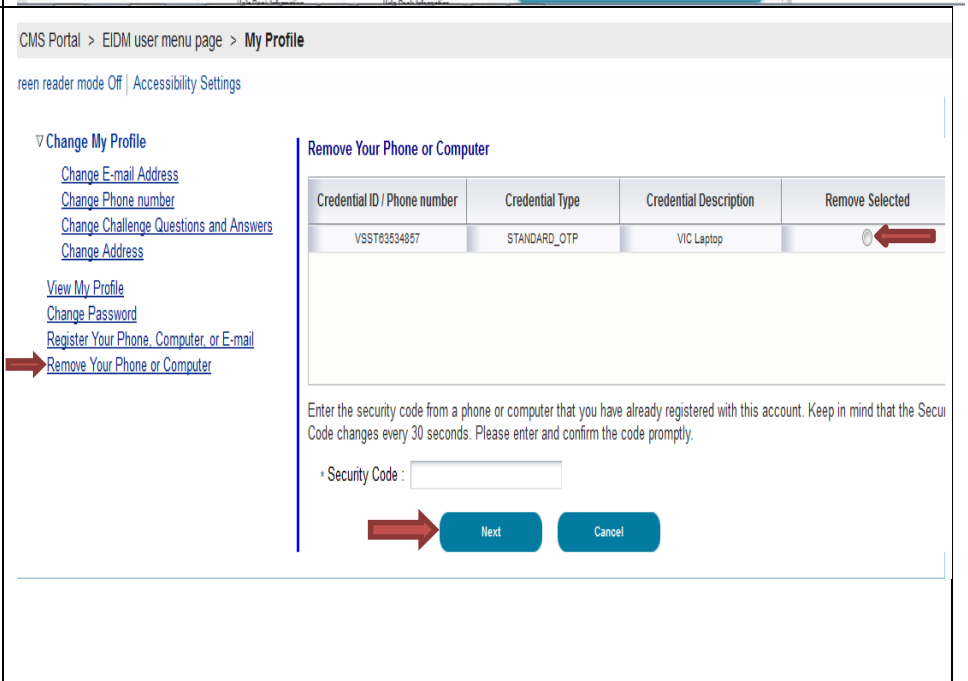
4. Select your username and then select **My Profile** from the drop-down menu to go to your profile.



5. Select **Remove Your Phone or Computer** from the left navigation links to begin the process of removing MFA device from your account.

Select the radio button next to the device you wish to remove, Enter the security code sent to your device and select **Next** to continue.

Note: The security code will be sent you the device you registered.



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

6. Your removal of registered **Multi Factor Authentication** device is now complete. Select **OK** to be directed to your profile page.

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


Remove Your Phone or Computer

You have successfully removed the registered Smartphone/Computer from your profile.



OK

4. Using MFA Login when accessing a MFA protected URL/Resource

Steps	Screenshots
<p>1. Go to https://portal.cms.gov/ and Select Login to CMS Secure Portal on the CMS Enterprise Portal.</p> <p>Note: The CMS Enterprise Portal supports the following internet browsers:</p> <ul style="list-style-type: none"> • Internet Explorer 8 • Internet Explorer 9 • Mozilla-Firefox • Chrome • Safari <p>Enable JavaScript and adjust any zoom features to ensure you are not seeing the screen in too wide of a view.</p>	

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

2. Read **Terms and Conditions** and select **I Accept** to continue.

Health Care Quality Improvement System

Provider Resources

Terms and Conditions

OMB No.0938-1236 | 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

3. Enter the following information and select **Log In**:

- EIDM User ID
- EIDM Password

CMS.gov | Enterprise Portal
Centers for Medicare & Medicaid Services

[Home](#) | [About CMS](#) | [Newsroom](#) | [Archive](#) | [?](#)

Health Care Quality Improvement System

Provider Resources

Welcome to CMS Enterprise Portal

User ID

Password



Log In

Cancel

[Forgot Password?](#)

[Forgot User ID?](#)

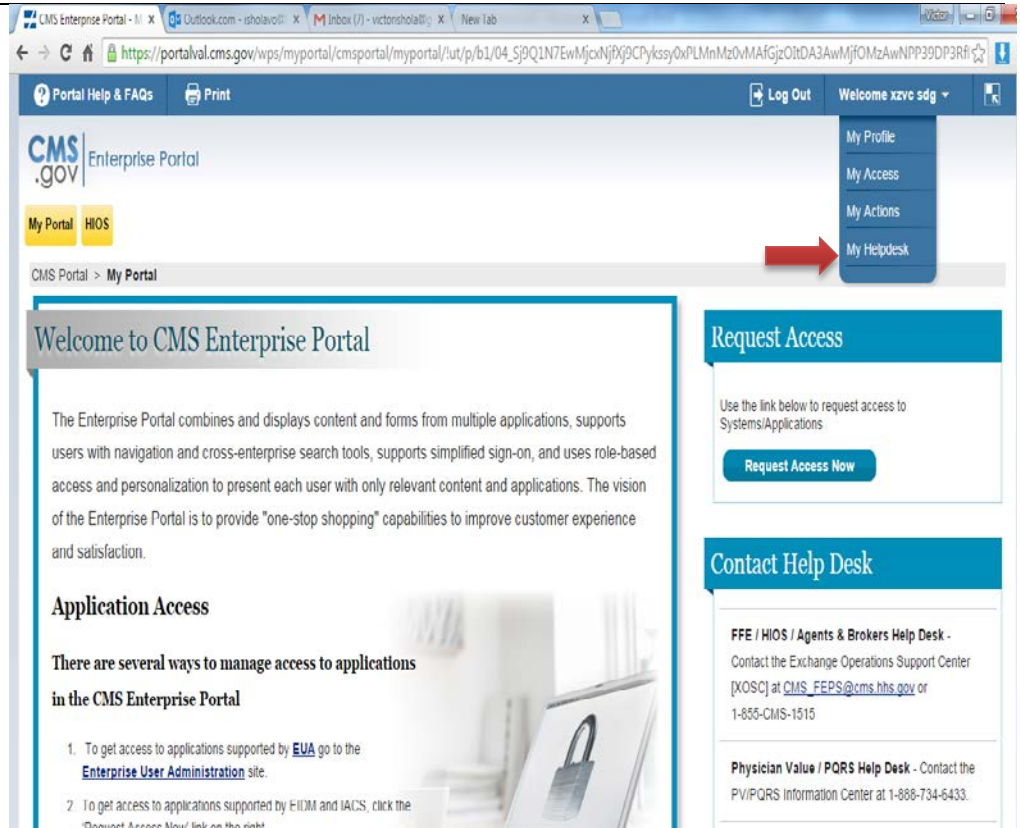
Need an account? Click the link - [New user registration](#)

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

4. Select a MFA protected resource/URL. You will be re-directed to the **Multi- Factor Terms and Conditions** screen in order to complete the second portion of the Multi-Factor Authentication process.

***Note:** We have used a sample 'My Helpdesk' URL for the purpose of this guide.*



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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

5. Read **Terms and Conditions** and select **I Accept** to continue.

Health Care Quality Improvement System Provider Resources

Terms and Conditions

OMB No.0938-1236 | 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

6. Enter your EIDM **UserID** and **Password** on the **Multi-Factor Authentication Login** screen and select **Login**.

CMS.gov Enterprise Portal
Centers for Medicare & Medicaid Services

Home | About CMS | Newsroom | Archive | ?

Health Care Quality Improvement System Provider Resources

Welcome to CMS Enterprise Portal

User ID

Password



Log In

Cancel

[Forgot Password?](#)

[Forgot User ID?](#)

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

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

CMS.gov Enterprise Portal Quick Reference Guide for Users adding Multi-Factor Authentication (MFA) to their existing Application Role

7. Select the **Credential Type** from the drop-down menu and then enter the **Security Code (VIP Token)** and then select **Log In**.

Note: You should select the credential type that you previously registered.

Welcome to CMS Enterprise Portal

Enter Security Code

A security code is required to access this page. When you originally requested access to this application the system required you to set up a Phone, Computer, or E-mail in order to retrieve a security code for Multifactor Authentication (MFA). If you did not complete the Multi-Factor Authentication(MFA) registration process, please select 'My Access' from the 'CMS Portal Home' page. Then, follow the necessary steps to complete the role request process. If you have completed the MFA set up process but are now having issues retrieving a security code please contact your application's help desk.

To retrieve a security code, please select the same credential type that you originally selected when first requesting access to the application from the drop down box(SMS,IVR or OTP). When entering the security code please enter it promptly as the code will expire for security purposes.

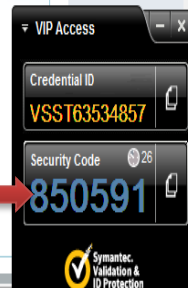
If you selected the E-mail One Time Password (OTP) option when you requested access to your application, please select that same credential type below to receive a security code via E-mail. The security code will be e-mailed to the e-mail address on your profile within 5 minutes. When entering the security code, please enter it promptly, as the security code will expire after 30 minutes or after it is used successfully the first time.

Credential Type: Phone/Tablet/PC/Laptop

Security Code (VIP Token)

Log In

Cancel



8. The **Multi-Factor Authentication** process is now complete. You will be redirected to your selected application page.

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