



Centers for Medicare & Medicaid Services

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

April 26, 2016
Version 00.01.00

Table of Contents

1. Introduction _____ 1

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

3. Remove a Registered Multi-Factor Authentication (MFA) Device _____ 12

4. Login Using MFA _____ 17

Table of Figures

Figure 1: CMS Enterprise Portal - Login to CMS Secure Portal	3
Figure 2: Terms and Conditions	3
Figure 3: Enter User ID	4
Figure 4: Register MFA Device	4
Figure 5: Register MFA Device - Select OK.....	5
Figure 6: Terms and Conditions	5
Figure 7: Enter User ID and Password	6
Figure 8: Challenge Questions.....	6
Figure 9: Select MFA Device Type.....	7
Figure 10: MFA Option (a) - Phone/Tablet/PC/Laptop.....	7
Figure 11: VIP Access Software.....	8
Figure 12: MFA Option (b) - Text Message - Short Message Service (SMS).....	8
Figure 13: MFA Option (c) - Voice Message - Interactive Voice Response (IVR)	9
Figure 14: MFA Option (d) - E-mail	10
Figure 15: Successful MFA Device Registration.....	10
Figure 16: Enter User ID	11
Figure 17: CMS Enterprise Portal - Login to CMS Secure Portal	12
Figure 18: Terms and Conditions	12
Figure 19: Enter User ID	13
Figure 20: Enter Password, Select MFA Device Type, Enter Security Code	13
Figure 21: CMS Enterprise Portal - My Profile	14
Figure 22: Remove Your Phone, Computer, or E-mail	14
Figure 23: Enter Security Code to Remove Your Phone, Computer, or E-mail.....	15
Figure 24: Successfully Removed Registered MFA Device	15
Figure 25: CMS Enterprise Portal - My Profile - Registered MFA Device.....	16
Figure 26: CMS Enterprise Portal - Login to CMS Secure Portal	17
Figure 27: Terms and Conditions	17
Figure 28: Enter User ID	18
Figure 29: Enter Password and Select MFA Device Type.....	18
Figure 30: VIP Access Software.....	19
Figure 31: MFA Device Type: Phone/Tablet/PC/Laptop.....	19
Figure 32: MFA Device Type: Interactive Voice Response (IVR)	19
Figure 33: MFA Device Type: One-Time Security Code.....	20
Figure 34: Unable to Access Security Code - Select OK.....	20
Figure 35: Enter User ID	21
Figure 36: Challenge Questions.....	21
Figure 37: Security Code Sent to E-mail - Select OK	21
Figure 38: E-mail with Security Code for MFA.....	22
Figure 39: Terms and Conditions	22
Figure 40: Enter User ID	22
Figure 41: Enter Password, Select MFA Device Type, Enter Security Code	23

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 the Health Insurance Oversight System (HIOS) can register for Multi-Factor Authentication (MFA), remove a registered MFA device, and log in with MFA.

Note: This guide is intended for existing HIOS users only. If you do not have an EIDM account or a HIOS account and would like to register for one, please visit <https://portal.cms.gov>.

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

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 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.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) 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, 9, 10, and 11
- Mozilla-Firefox
- Chrome
- Safari



Figure 1: CMS Enterprise Portal - Login to CMS Secure Portal

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

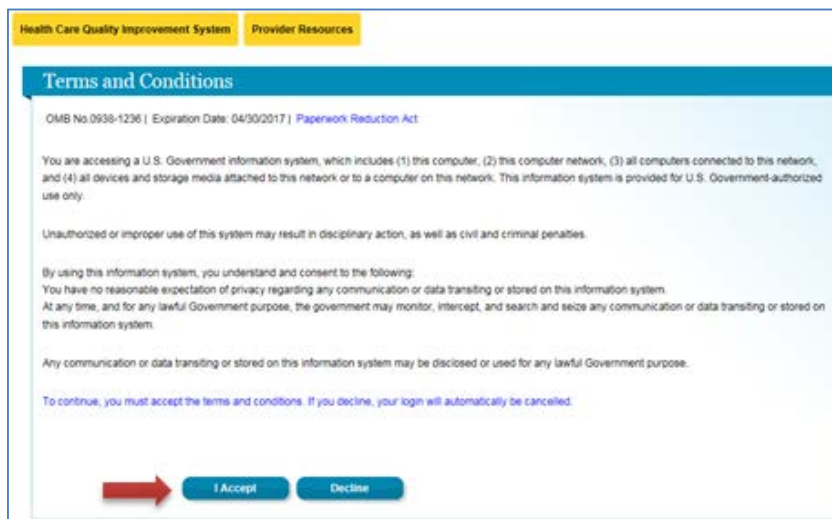


Figure 2: Terms and Conditions

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

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



Figure 3: Enter User ID

4. Select the **Register MFA Device** link.

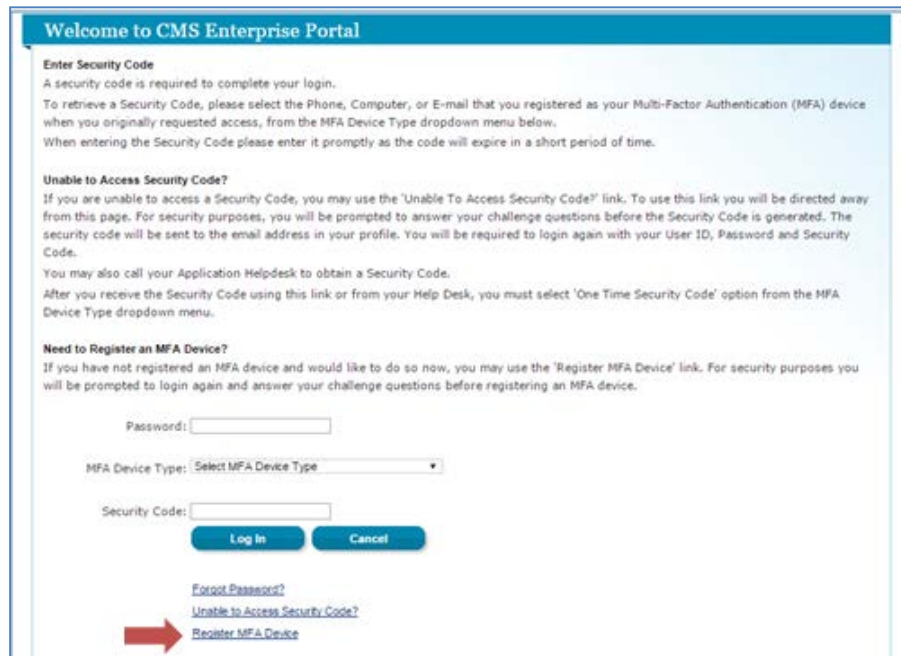


Figure 4: Register MFA Device

5. Select **OK** to navigate away from the login page.

Note: Selecting **Cancel** will end the process to register an MFA Device.

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

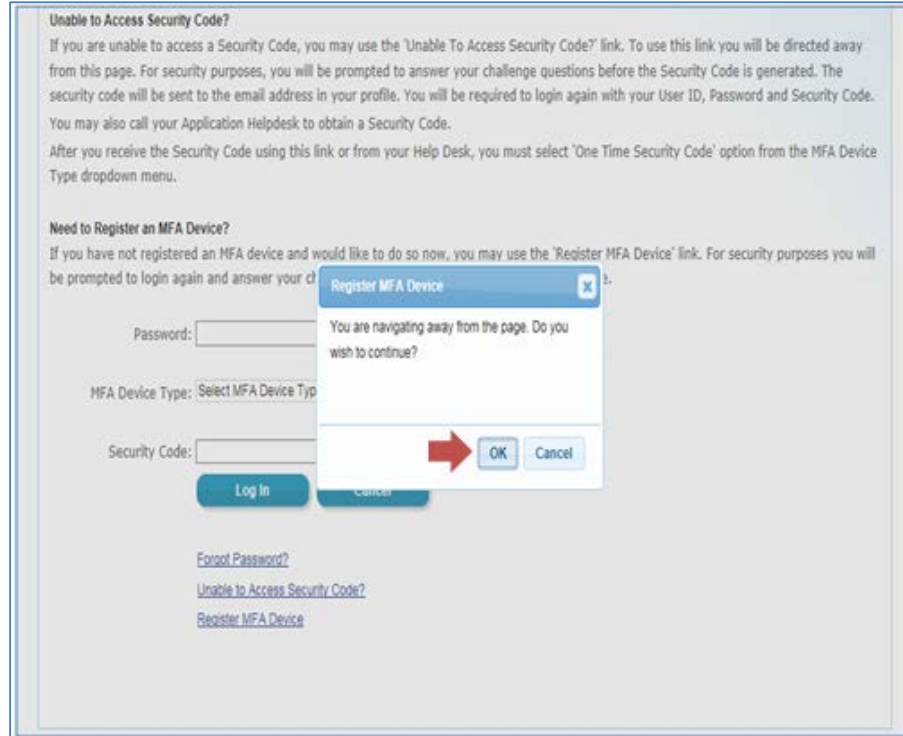


Figure 5: Register MFA Device - Select OK

6. Read the Terms and Conditions and select **I Accept**.

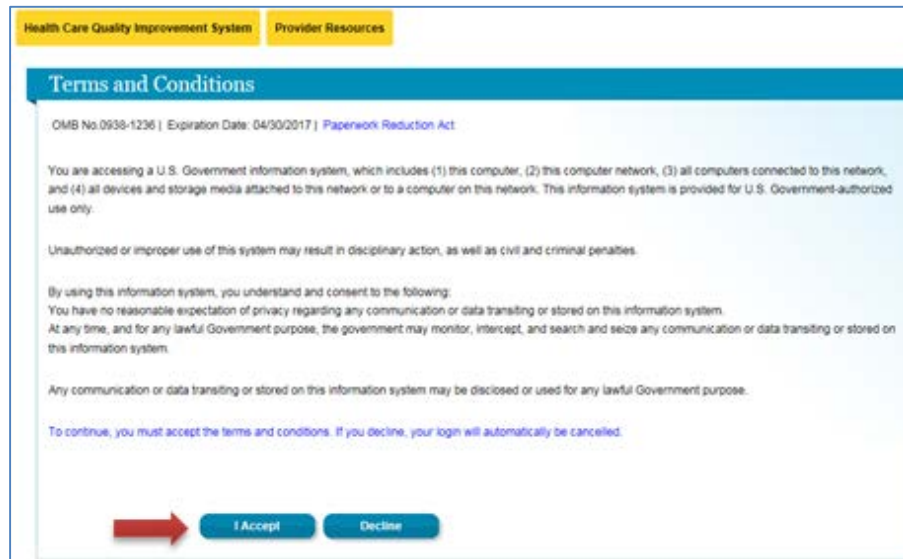


Figure 6: Terms and Conditions

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

7. Enter your **User ID** and **Password**, and select **Log In**.



Figure 7: Enter User ID and Password

8. Answer the challenge questions and select **Next**.

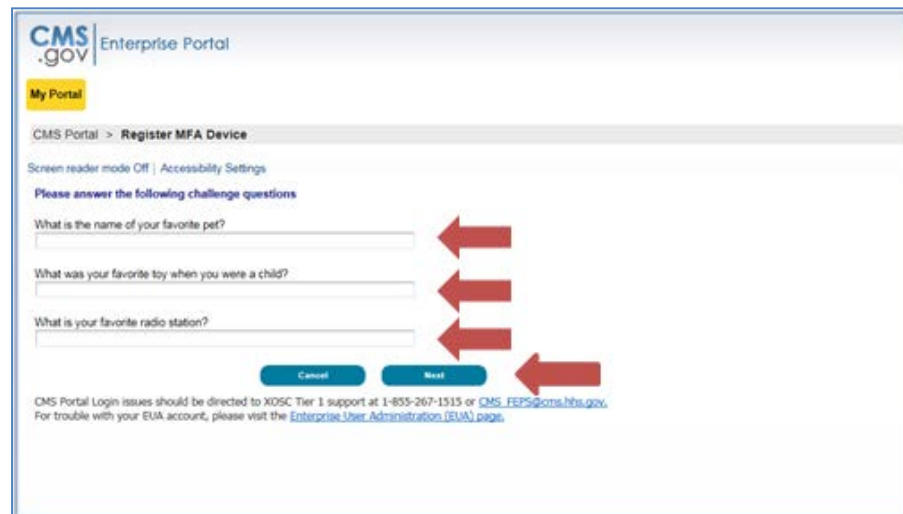


Figure 8: Challenge Questions

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

9. Select an MFA device from the **MFA Device Type** dropdown.

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

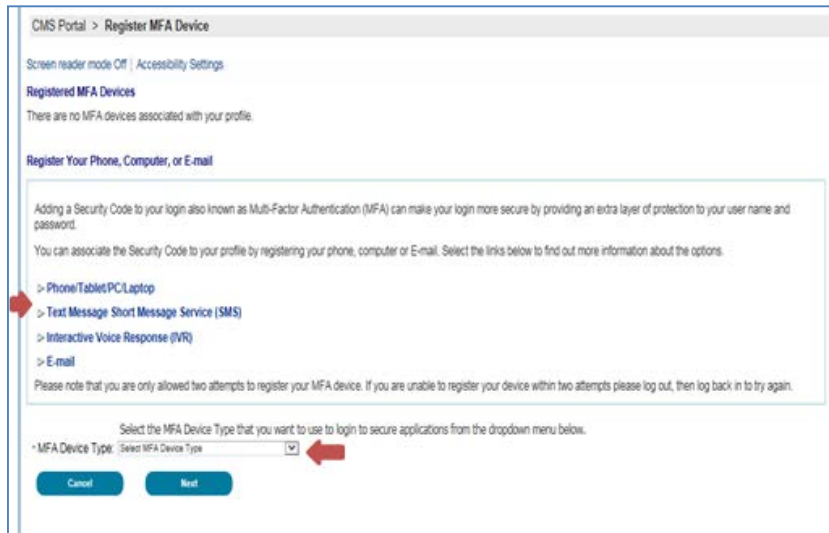


Figure 9: Select MFA Device Type

9(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 (e.g., Laptop) in the field labeled **MFA Device Description**. Then select **Next**.

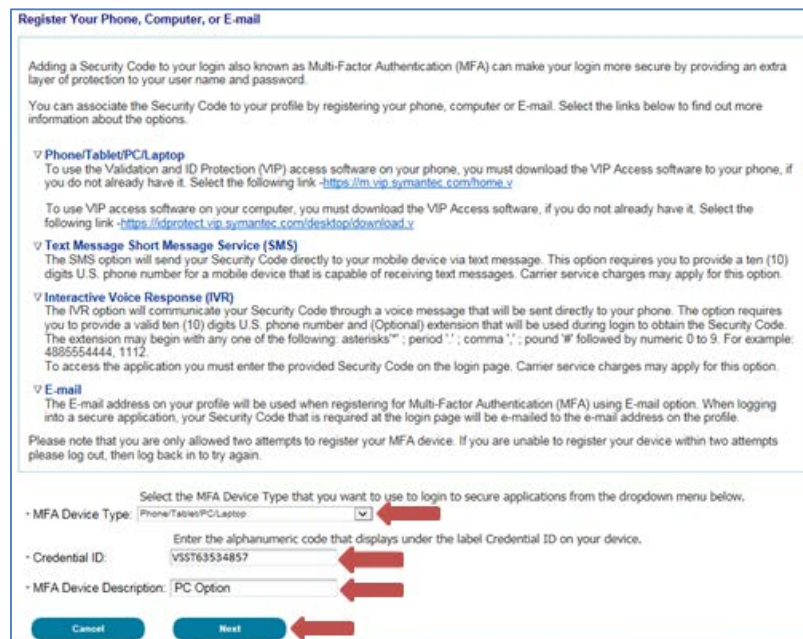


Figure 10: MFA Option (a) - Phone/Tablet/PC/Laptop

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

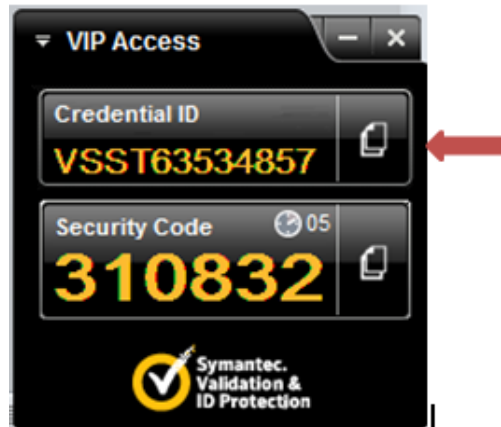


Figure 11: VIP Access Software

OR

9(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 (e.g., Text) in the field labeled **MFA Device Description** and 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: 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: ▼

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

• Phone Number:

• MFA Device Description:

Figure 12: MFA Option (b) - Text Message - Short Message Service (SMS)

OR

9(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 (e.g., IVR) in the field labeled **MFA Device Description** and select **Next**.

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

The screenshot shows a web form titled "Register Your Phone, Computer, or E-mail". It contains several sections of text and form fields. The "Interactive Voice Response (IVR)" section is highlighted with a red box. Below this section, there are form fields for "MFA Device Type" (set to "Interactive Voice Response (IVR)"), "Phone Number" (807 345 2423), "Extension" (242), and "MFA Device Description" (IVR). There are also "Cancel" and "Next" buttons at the bottom. Red arrows point to the "MFA Device Type" dropdown, the "Extension" field, the "MFA Device Description" field, and the "Next" button.

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: 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: Interactive Voice Response (IVR) ▼

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

Phone Number: 807 345 2423 Extension: 242

MFA Device Description: IVR

Cancel Next

Figure 13: MFA Option (c) - Voice Message - Interactive Voice Response (IVR)

OR

9(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 (e.g., 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.

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: E-mail

E-mail Address: laluru@qssinc.com

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: E-mail

Cancel Next

Figure 14: MFA Option (d) - E-mail

10. Your registration for the **Multi-Factor Authentication** is now complete. Select **OK** to continue to log in with MFA.

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

CMS.gov Enterprise Portal
Centers for Medicare & Medicaid Services
Health Care Quality Improvement System Provider Resources
Learn about your healthcare options

CMS Portal > Register MFA Device

Screen reader mode Off / Accessibility Settings

Register Your Phone, Computer, or E-mail

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

Click "OK" to close this window and login.

OK

Figure 15: Successful MFA Device Registration

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

11. Enter your **User ID** and select **Next** to continue to log in.

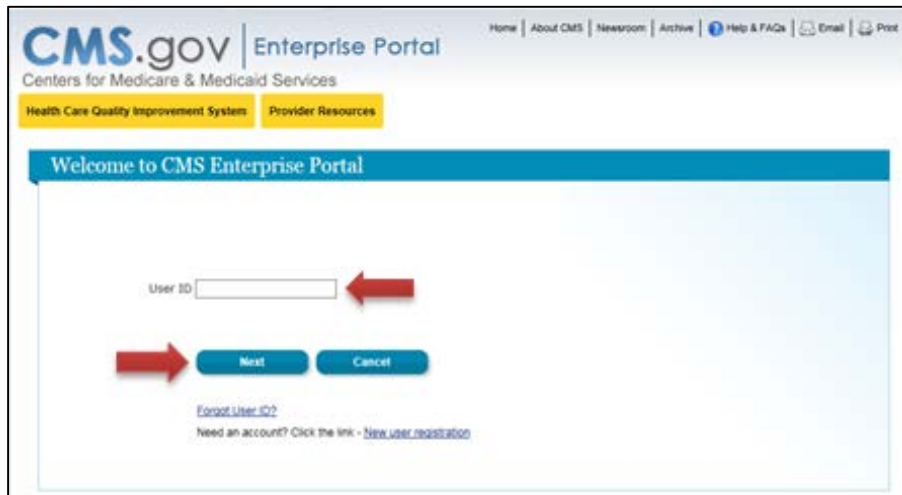


Figure 16: Enter User ID

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.

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, 9, 10, and 11
- Mozilla-Firefox
- Chrome
- Safari



Figure 17: CMS Enterprise Portal - Login to CMS Secure Portal

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

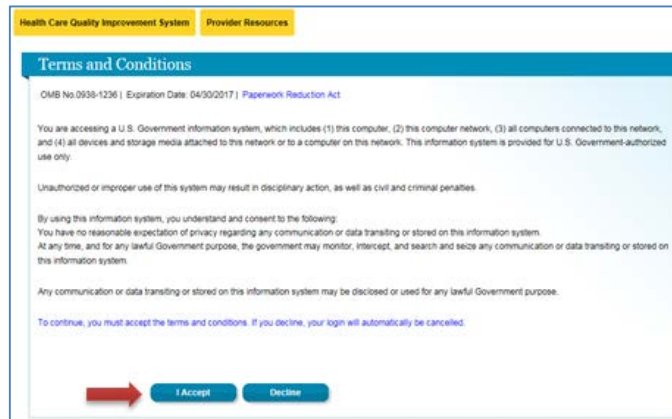
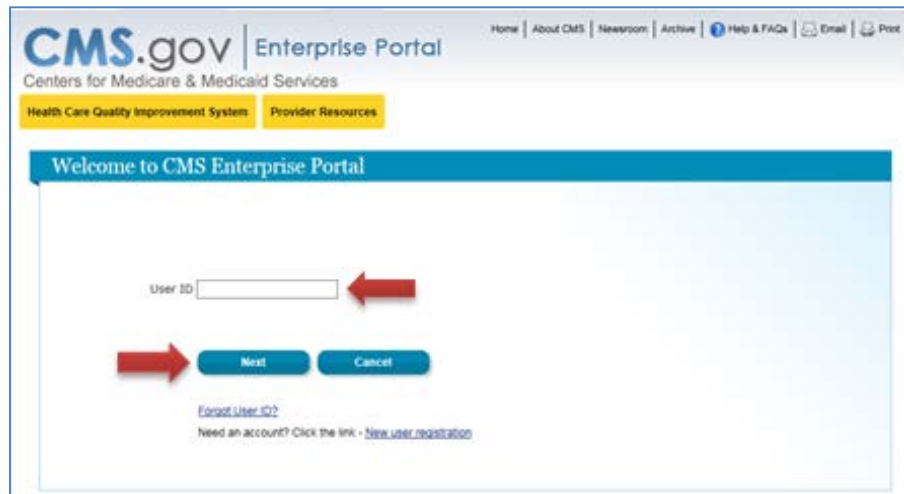


Figure 18: Terms and Conditions

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

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

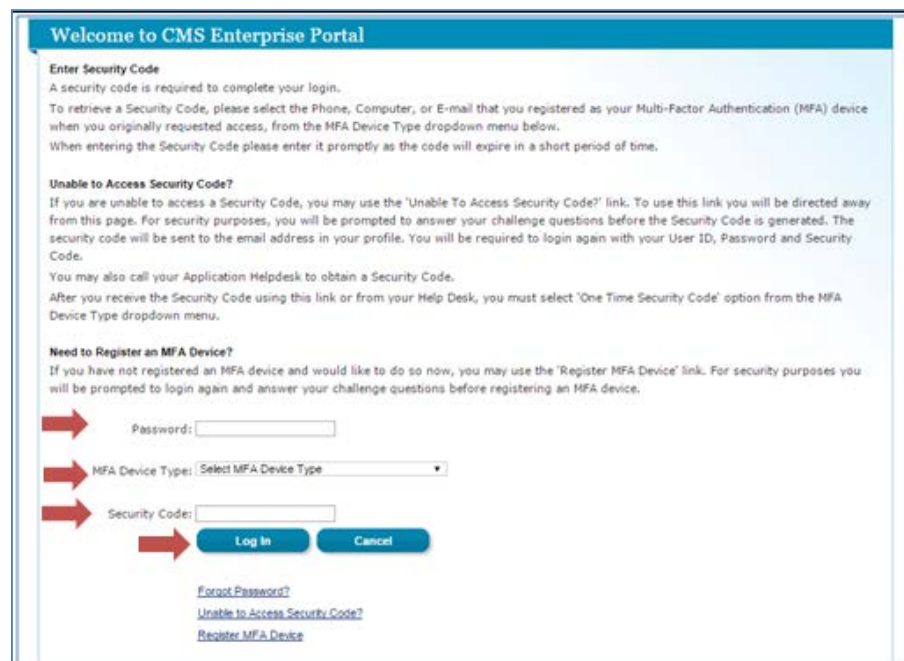


The screenshot shows the CMS.gov Enterprise Portal login page. At the top, there is a navigation bar with links for Home, About CMS, Newsroom, Archive, Help & FAQs, Email, and Print. Below this is the CMS.gov logo and the text "Enterprise Portal" and "Centers for Medicare & Medicaid Services". There are two yellow buttons: "Health Care Quality Improvement Systems" and "Provider Resources". A blue banner reads "Welcome to CMS Enterprise Portal". The main content area has a "User ID" input field with a red arrow pointing to it. Below the input field are "Next" and "Cancel" buttons, with a red arrow pointing to the "Next" button. There are also links for "Forgot User ID?" and "Need an account? Click the link - New User 092323500".

Figure 19: Enter User ID

4. Enter your **Password**, select an MFA device from the **MFA Device Type** dropdown, enter the **Security Code**, and select **Log In**.

Note: You should select the **MFA Device Type** that you previously registered.



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 this is the CMS.gov logo and the text "Enterprise Portal" and "Centers for Medicare & Medicaid Services". There are two yellow buttons: "Health Care Quality Improvement Systems" and "Provider Resources". A blue banner reads "Welcome to CMS Enterprise Portal". The main content area has a section titled "Enter Security Code" with instructions. Below this are three input fields: "Password:", "MFA Device Type: Select MFA Device Type", and "Security Code:". There are red arrows pointing to each of these fields. Below the input fields are "Log In" and "Cancel" buttons, with a red arrow pointing to the "Log In" button. There are also links for "Forgot Password?", "Unable to Access Security Code?", and "Register MFA Device".

Figure 20: Enter Password, Select MFA Device Type, Enter Security Code

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

5. Select your username and then select **My Profile** from the dropdown menu to go to your profile.

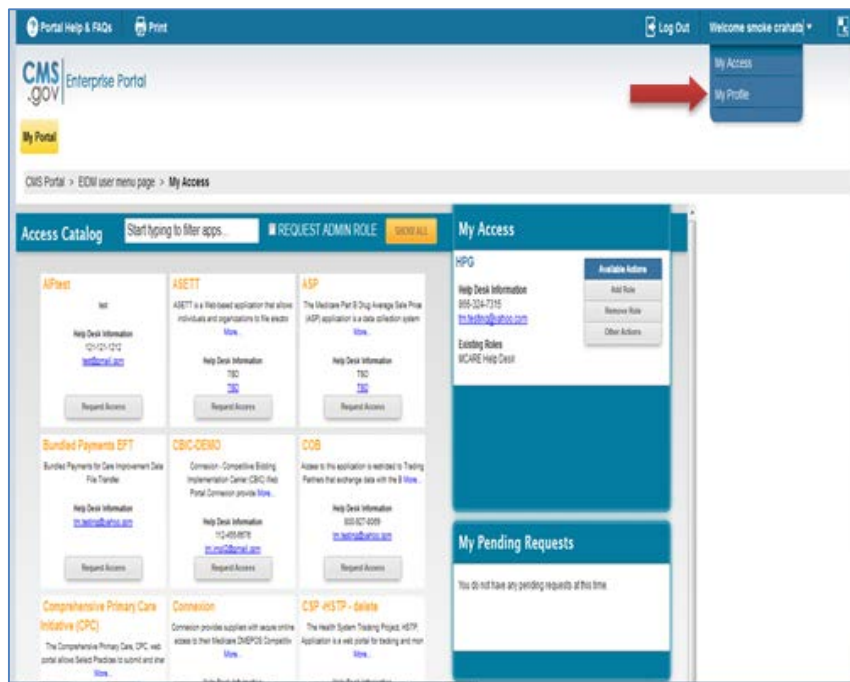


Figure 21: CMS Enterprise Portal - My Profile

6. Select the **Remove Your Phone, Computer, or E-mail** link to remove a registered MFA device from your profile. 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.

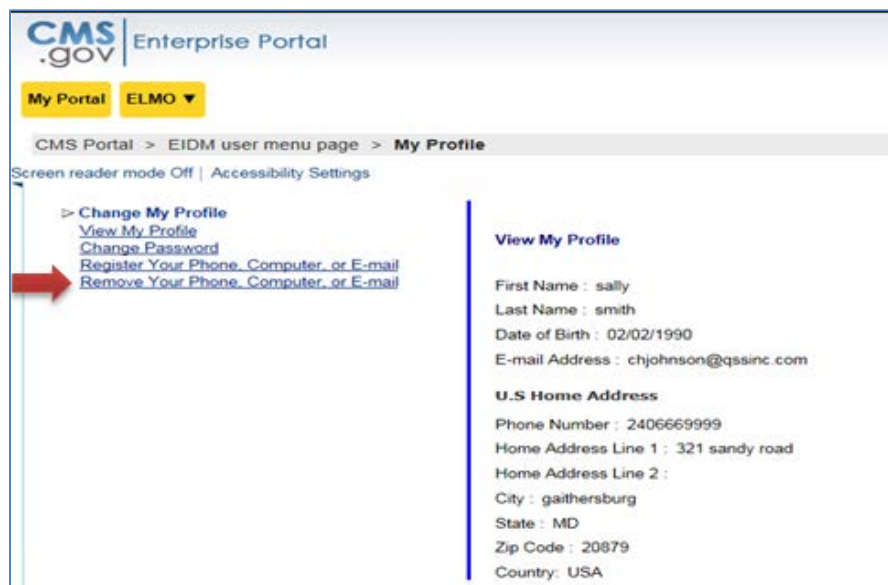


Figure 22: Remove Your Phone, Computer, or E-mail

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

7. 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.

Note: Selecting **Cancel** will end the device removal process.

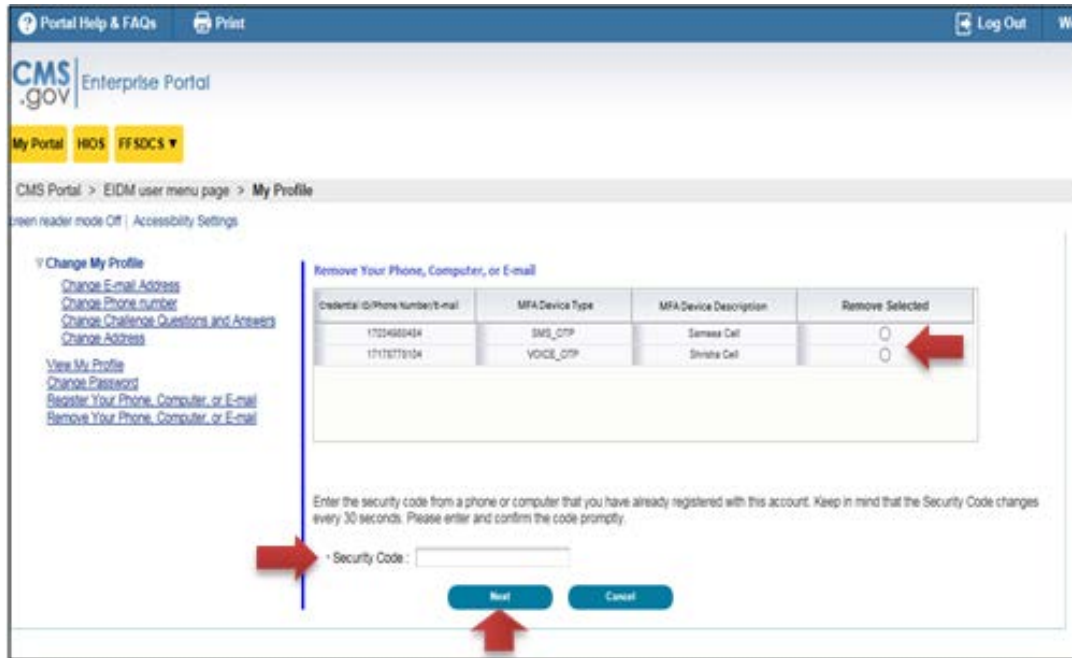


Figure 23: Enter Security Code to Remove Your Phone, Computer, or E-mail

8. Removal of your registered MFA device is now complete. Select **OK** to proceed.

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



Figure 24: Successfully Removed Registered MFA Device

9. You will need at least one MFA device registered to your profile to continue to access your application using MFA. To remove the last registered device from your profile, you will need to register a new device to your profile.

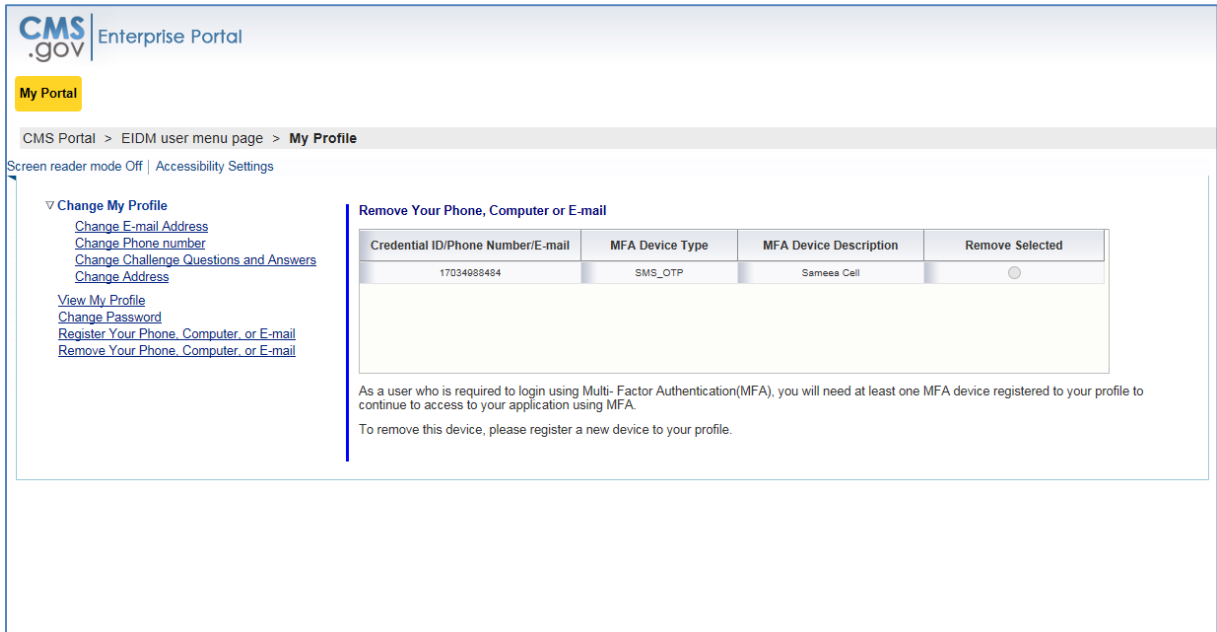


Figure 25: CMS Enterprise Portal - My Profile - Registered MFA Device

4. Login Using MFA

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, 9, 10, and 11
- Mozilla-Firefox
- Chrome
- Safari



Figure 26: CMS Enterprise Portal - Login to CMS Secure Portal

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

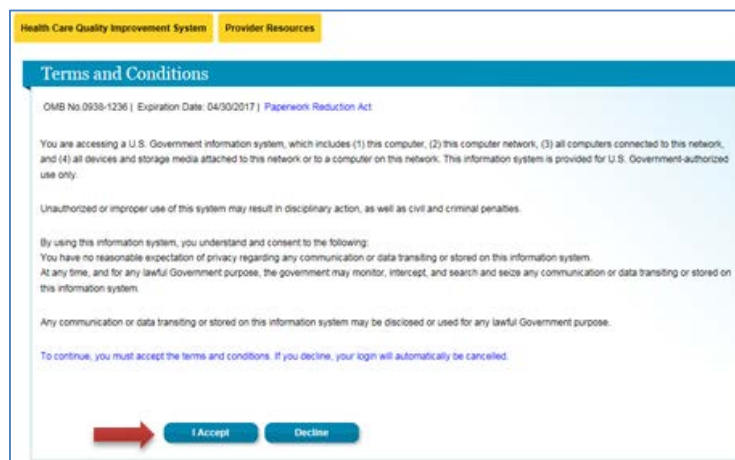


Figure 27: Terms and Conditions

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

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

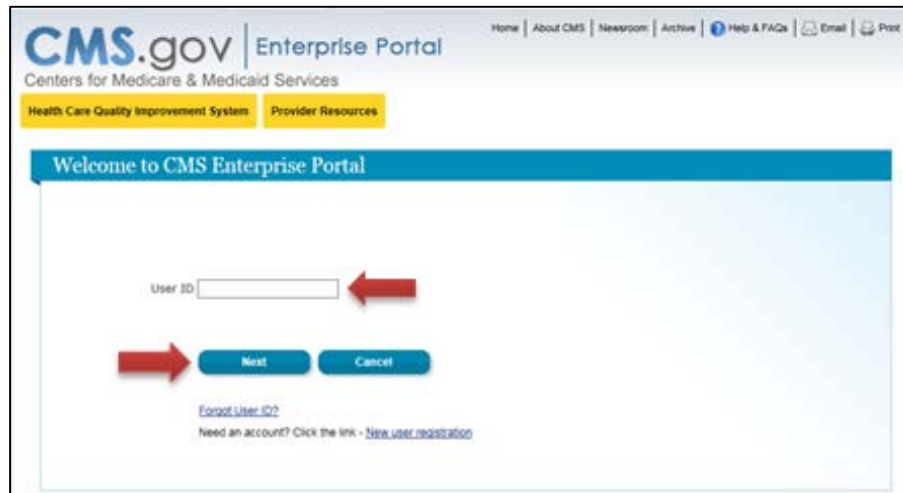


Figure 28: Enter User ID

4. Enter your **Password**, select an MFA device from the **MFA Device Type** dropdown, 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.

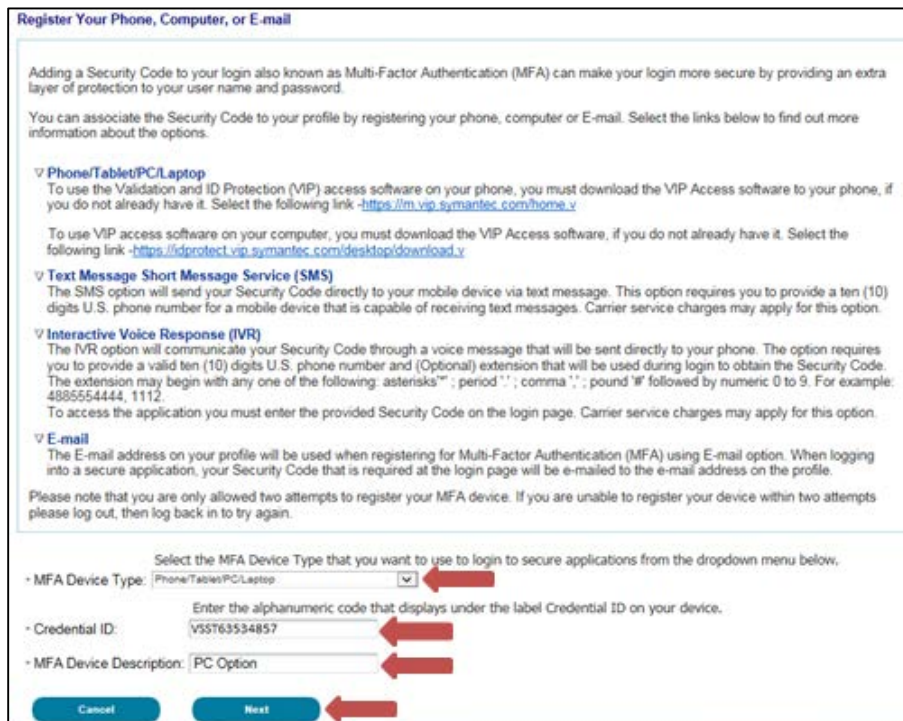


Figure 29: Enter Password and Select MFA Device Type

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

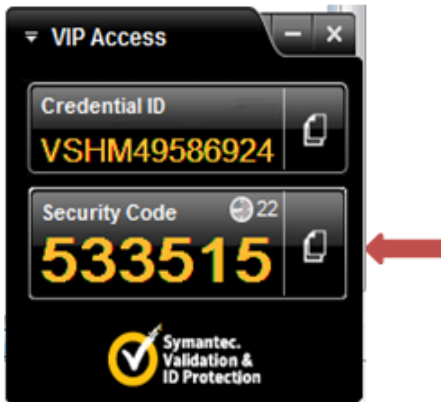


Figure 30: VIP Access Software

4(a). If you select **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**.



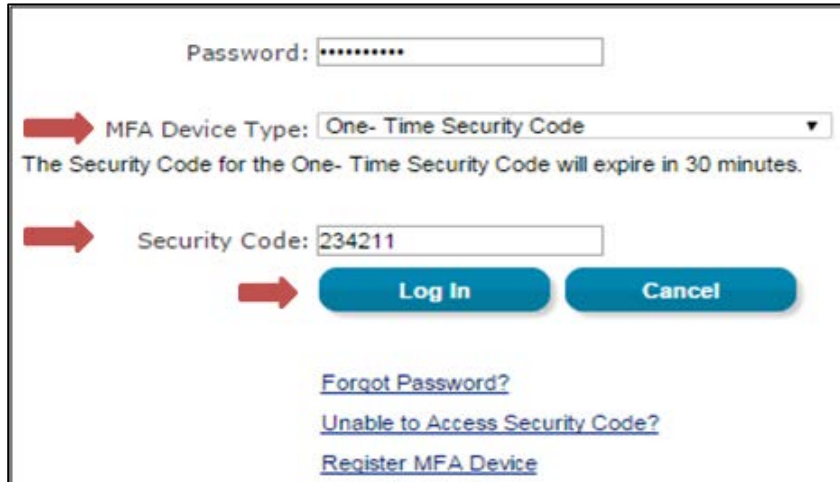
Figure 31: MFA Device Type: Phone/Tablet/PC/Laptop

4(b). If you select **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**.



Figure 32: MFA Device Type: Interactive Voice Response (IVR)

4(c). If you select **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**.

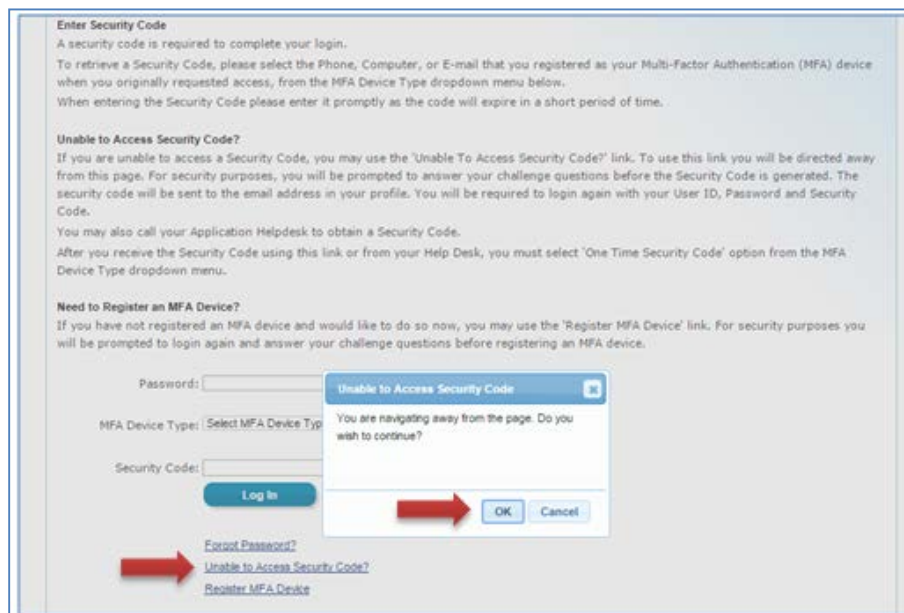


The screenshot shows a login form with the following elements:

- A "Password:" field with a masked password "*****".
- An "MFA Device Type:" dropdown menu set to "One-Time Security Code". A red arrow points to this dropdown.
- A message: "The Security Code for the One-Time Security Code will expire in 30 minutes."
- A "Security Code:" field containing the code "234211". A red arrow points to this field.
- "Log In" and "Cancel" buttons. A red arrow points to the "Log In" button.
- Links for "Forgot Password?", "Unable to Access Security Code?", and "Register MFA Device".

Figure 33: MFA Device Type: One-Time Security Code

5. If you are not able to access your Security Code, select the '**Unable to Access Security Code?**' link. On selecting this link, the '**Unable to Access Security Code?**' popup message will be displayed. Select **OK** to continue



The screenshot shows a login page with a popup message. The background page includes:

- Fields for "Password:", "MFA Device Type:" (set to "Select MFA Device Type"), and "Security Code:".
- "Log In" and "Cancel" buttons.
- Links for "Forgot Password?", "Unable to Access Security Code?", and "Register MFA Device". A red arrow points to the "Unable to Access Security Code?" link.

The popup message is titled "Unable to Access Security Code" and contains the following text:

You are navigating away from the page. Do you wish to continue?

Buttons for "OK" and "Cancel" are at the bottom of the popup. A red arrow points to the "OK" button.

Figure 34: Unable to Access Security Code - Select OK

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

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

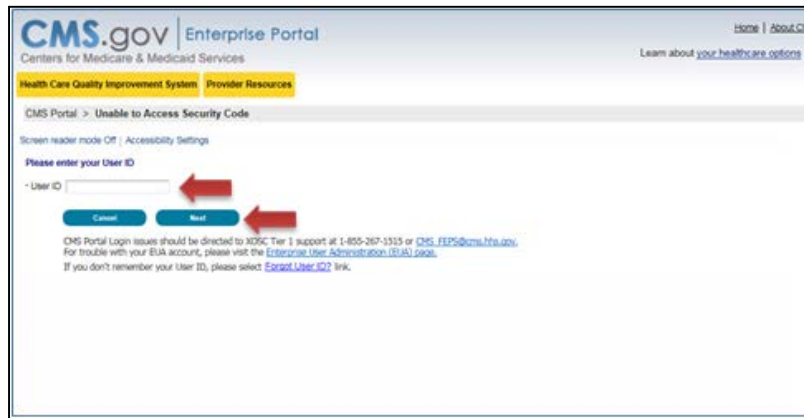


Figure 35: Enter User ID

7. Answer the challenge questions and select **Next**.



Figure 36: Challenge Questions

8. Select **OK** to return to the login page.

Note: This security code will expire in 30 minutes or after it is used successfully for the first time.

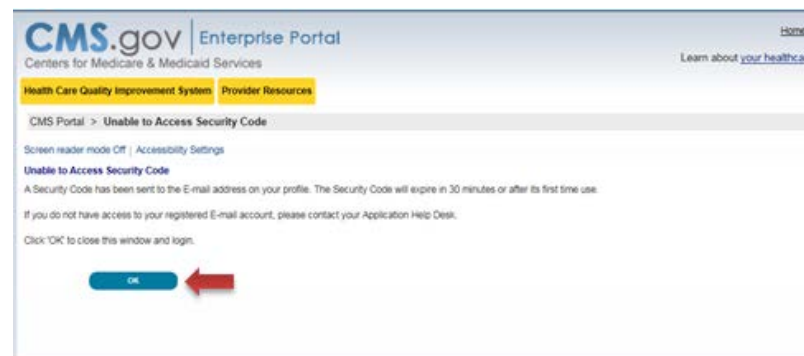


Figure 37: Security Code Sent to E-mail - Select OK

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to their Health Insurance Oversight System (HIOS) Application Role

9. An e-mail with the Security Code will be sent to the E-mail address on your profile.

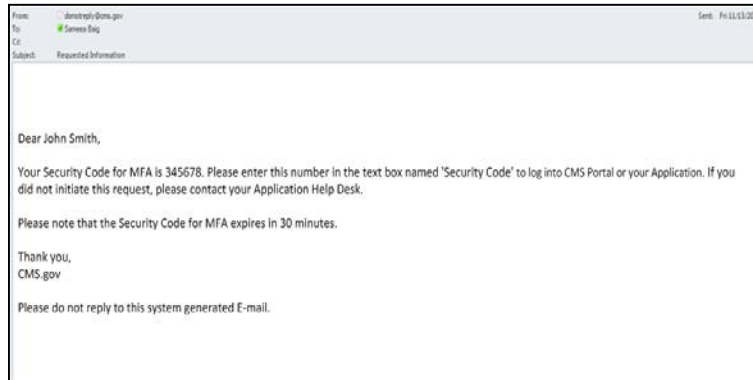


Figure 38: E-mail with Security Code for MFA

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

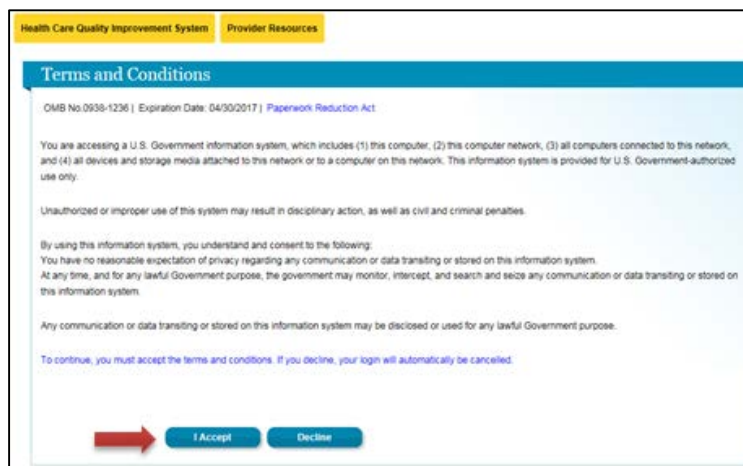


Figure 39: Terms and Conditions

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

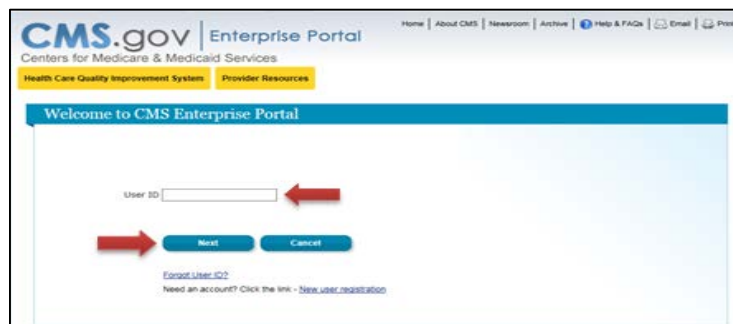


Figure 40: Enter User ID

If you have questions about or need assistance regarding MFA, please contact the Exchange Operations Support Center (XOSC) at CMS_FEPS@cms.hhs.gov or 1-855-267-1515.

12. Enter your **Password**, select **One-Time Security Code** as the **MFA Device Type**, and enter the **Security Code** that was sent to the E-mail address on your profile. Then select **Log In**.

The screenshot shows the 'Welcome to CMS Enterprise Portal' page. It includes instructions for entering a security code and links for 'Forgot Password?', 'Unable to Access Security Code?', and 'Register MFA Device'. The login form has the following fields and options:

- Header: Health Care Quality Improvement System | Provider Resources
- Title: Welcome to CMS Enterprise Portal
- Section: Enter Security Code
- Text: A Security Code is required to complete your login. To retrieve a Security Code, please select the Phone, Computer, or E-mail that you registered as your Multi-Factor Authentication (MFA) device when you originally requested access, from the MFA Device Type dropdown menu below.
- Text: When entering the Security Code, please enter it promptly as the code will expire in a short period of time.
- Section: Unable to Access Security Code?
- Text: If you are unable to access a Security Code, you may use the 'Unable To Access Security Code?' link. To use this link you will be directed away from this page. For security purposes, you will be prompted to answer your challenge questions before the Security Code is generated. The Security Code will be sent to the email address in your profile. You will be required to login again with your User ID, Password and Security Code.
- Text: You may also call your Application Help Desk to obtain a Security Code.
- Text: After you receive the Security Code using this link or from your Help Desk, you must select the 'One-Time Security Code' option from the MFA Device Type dropdown menu.
- Section: Need to Register an MFA Device?
- Text: If you have not registered an MFA device and would like to do so now, you may use the 'Register MFA Device' link. For security purposes you will be prompted to login again and answer your challenge questions before registering an MFA device.
- Form fields:
 - Password: [masked]
 - MFA Device Type: One-Time Security Code
 - Text: The security code for the Phone/Tablet/PC Laptop will expire in 10 minutes.
 - Security Code: 345678
 - Buttons: Log In, Cancel
- Links: [Forgot Password?](#), [Unable to Access Security Code?](#), [Register MFA Device](#)

Figure 41: Enter Password, Select MFA Device Type, Enter Security Code