

Centers for Medicare & Medicaid Services

|  |
| --- |
| **CMS Enterprise Portal Quick Reference Guide (QRG)**  **Multi-Factor Authentication (MFA) Optional** |
| January 13, 2017  Version 1.4 Final |

**Table of Contents**

[1. Introduction 2](#_Toc472070674)

[2. Step-by-Step Instructions to Request a Role 3](#_Toc472070675)

[3. Multi-Factor Authentication (MFA) Optional 6](#_Toc472070676)

[Add MFA 6](#_Toc472070677)

[Skip MFA 9](#_Toc472070678)

[4. Step-by-Step Instructions to Log In with MFA 10](#_Toc472070679)

[5. Remove MFA Registration 13](#_Toc472070680)

[6. Step-by-Step Instructions for Existing Users Adding MFA 14](#_Toc472070681)

# Introduction

This guide provides step-by-step instructions on how users with an active CMS 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 Enterprise Portal account and want to register for one, visit* [*https://portal.cms.gov*](https://portal.cms.gov)*.*

# **Step-by-Step Instructions to Request a Role**

This section outlines the steps users take to request a role. Please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 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 browsers: Internet Explorer 11, Firefox, Chrome, and Safari*. | Portal Landing Page |
| 1. Read the ‘Terms and Conditions’ pageand select **I Accept**to continue. | I Accept the Terms and Conditions |
| 1. Enter your **User ID** and select **Next**. | Enter User ID |
| 1. Enter your **Password** and select **Log In**. | Enter password and select Log In. |
| 1. Select **Request Access Now** in the ‘Request Access’ **section** to begin the process of requesting a new user role.   ***Note:*** *You may also locate the ‘Welcome <First> <Last>’ drop-down list in the top-right corner of the page and select* ***My Access*** *to begin the process of requesting a new user role.* | Request Access Now link |
| 1. Look for your application in the Access Catalog and select **Request Access*.*** | Access Catalog |
| 1. 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.* | Request New Application Access |
| 1. 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.* | Identity Verification |
| 1. Remote Identity Proofingis now complete. Select **Next** to proceed to optional registration for MFA. | Complete Step Up |

# Multi-Factor Authentication (MFA) Optional

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 e-mail 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.

## Add MFA

During a role request, users may have the option to add MFA to their profile or skip this process. This section outlines the steps to complete the process of adding MFA to your user profile. Please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 1. Select **Add MFA** to begin device setup for the Multi-Factor Authenticationlogin. | Multi Factor Authenication Information |
| 1. Select an MFA device from the **MFA Device Type**drop-down. Then select **Next**.   ***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.*  ***Cancel:*** *Selecting this will end the role request.* | Register your Phone, Computer, or E-mail |
| 2a. 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**. | Select the MFA Device that you want to use to log into your application.  VIP Access |
| 2b. 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**. | Selecting Text Message - Short Message Service (SMS) as the MFA device type. |
| 2c. 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.* | Selecting Voice Message Interactive Voice Response (IVR) as the MFA device type |
| 2d. 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.* | Selecting E-mail as the MFA device type |
| 1. Your registration for **Multi-Factor Authentication** is now complete. Select **Next** to complete the role request process. | Complete role request. |
| 1. If the role requires approval, a message will display with a tracking number for your request. An e-mail will be sent once your request has been approved or rejected. Select **OK**to continue. | Message with tracking number |

## Skip MFA

The next section will go through the steps to skip registering a device for MFA via “Skip MFA”. Please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 1. Select **Skip MFA** to begin device setup for the **Multi-Factor Authentication** login. | Skip MFA button |
| 1. If the role requires approval, a message will display with a tracking number for your request. An e-mail is sent once your request has been approved or rejected. Select **OK** to continue. | Message with tracking number |

# Step-by-Step Instructions to Log In with MFA

The login experience will be different once an MFA Device has been registered to your user profile. Please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 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 browsers: Internet Explorer 11, Firefox, Chrome, and Safari*. | Portal Landing Page |
| 1. Read the ‘Terms and Conditions’ pageand select **I Accept**to continue. | I Accept the Terms and Conditions |
| 1. Enter your **User ID** and select **Next**. | Enter User ID |
| 1. 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 after 30 minutes. The Security Code for the other MFA device types will expire after 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.* | Enter password, select MFA device, and select Log In. |
| 4a. If you select **Phone/Tablet/PC/ Laptop** as the ‘MFA Device Type’, enter the VIP Access software’s ‘Security Code’ as the MFA **Security Code** and select **Log In**. | VIP Access  Enter Security Code |
| 4b. If you select **Text Message – Short Message Service (SMS)**, **Interactive Voice Response (IVR)**,or **E-mail** as the **‘**MFA Device Type’,select **Send** to receive the code on the selected MFA device type.  Enter the code in the **Security Code** field and select **Log In**. | Enter Security Code |
| 4c. If you select **One-Time Security Code** as the **‘**MFA Device Type’, enter the code you receive either in the e-mail sent to your registered e-mail address via the ‘Unable to Access Security Code?’ link or from your Application Help Desk in the **Security Code** field and select **Log In**. | Enter Security Code |

# Remove MFA Registration

Users may remove the MFA option 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 complete MFA in order to log in. Please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 1. Select the **Remove Your Phone, Computer, or E-mail** link to remove a registered MFA device from your profile. | Remove Your Phone, Computer, or E-mail link |
| 1. 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.* | Remove Your Phone, Computer, or E-mail page |
| 1. 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.* | Select OK to remove the MFA device. |
| 1. Once the MFA Device is removed from your user profile, a confirmation e-mail will be sent to the registered e-mail address in your user profile. | Email confirming removal of MFA device |

# 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 each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 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 browsers: Internet Explorer 11, Firefox, Chrome, and Safari*. | Portal Landing Page |
| 1. Read the ‘Terms and Conditions’ pageand select **I Accept**to continue. | I Accept the Terms and Conditions |
| 1. Enter your **User ID** and select **Next**. | Enter User ID |
| 1. Enter your **Password** and select **Log In**. | Enter password and select Log In. |
| 1. Locate the ‘Welcome <First> <Last>’ drop-down list in the top-right corner of the page and select **My Profile**. | Select My Profile from the drop-down menu |
| 1. Select the **Register Your Phone, Computer, or E-mail** link to register an MFA device to your profile. | Register Your Phone, Computer, or E-mail link |
| 1. 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.* | Register your phone, computer, or e-mail |
| 7a. 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**. | Selecting Phone/Table/PC/Laptop as the MFA device type.  VIP Access |
| 7b 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**. | **Selecting Text Message - Short Message Service (SMS) as the MFA device type** |
| 7c. If selecting **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 (e.g., 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*. | Interactive Voice Response (IVR) as the MFA device type |
| 7d. 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.* | Selecting E-Mail as the MFA device type |
| 1. 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.* | Complete MFA registration |