**CMS IDM
Multi-Factor Authentication (MFA) DEVICE Registration**

# Introduction

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

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

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

* **Smart Phone**: Users can download Okta Verify and Google Authenticator access software on their smart phone/tablet. The user is required to enter the one-time passcode (OTP) generated by the respective client.
* **Short Message Service (SMS)**: Users can use the SMS option to have their Security Code texted to their phone. The user must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
* **Interactive Voice Response (IVR)**: The user can select the IVR option to receive a voice message containing their Security Code. The user must provide a valid phone number and (optional) phone extension.
* **E-mail**: Users can select the E-mail option to receive an E-mail containing the Security Code required at login. The E-mail address on the user’s profile will be used.

*Note: Delays in E-mail transmission, spam filters, and other issues outside the user’ control can make this the least desirable option to receive a security code.*

# User Instructions

To gain access to a CMS MFA protected application, follow these steps

| **Step** | **Action** |
| --- | --- |
| **Step 1** | If you select a CMS MFA Protected application, you will first be directed to the **Multi-Factor Authentication Information** page. Select **Register a Device**, to begin the MFA Registration process. This picture displays the process of registering a MFA device on the Multi-Factor Authentication Information page. Select register a device to begin the MFA Registration process. |
| **Step 2** | To make your account more secure, you will be directed to the **Manage MFA Devices** page. Select the **MFA Device Type** you wish to register from the drop-down menu.This picture displays the drop-down menu options for each MFA device type. Select the MFA device type from the drop-down menu.***Notes:******For Google Authenticator and Okta Very Client****: Enter the Credential ID generated by the Google/Authenticatir Access client.****For Text****: You will be asked to enter a valid phone number to receive your Security Code.****For Interactive Voice Response (IVR)****: Enter the 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.* ***, (comma)*** *Creates a short delay of approximately 2 seconds;* ***. (period)*** *Creates a longer delay of approximately 5 seconds;* ***\*(asterisks)*** *Used by some phone systems to access an extension; and* ***# (pound/hash)*** *Used by some phone systems to access an extension.**You may use a comma if you are not sure of the special character supported by your company’s phone system.****For E-mail****: The E-mail on your profile will be used to send the Security Code required at login.* |
| **Step 2a** | **Using theText Message (SMS)** Follow these steps to use Text Message (SMS): 1. Enter your phone number and select send code

This picture displays the first step in using text messaging (SMS) or SMS option to send a security code directly to the users mobile device. Enter your phone number and select send code.  |
| **Step 3** | Enter the security code received and select add Device…This picture displays the second step in using text messaging (SMS) or SMS option when receiving a security code on the users mobile device. Further, it describes the process of entering the security code in the MFA application on the users mobile device. Enter the security code received and select add device.  |
| **Step 4** | After submitting the registration, a message will be displayed that you have successfully registered your device.This picture displays the confirmation page and notice the user should receive upon successsful MFA device registration, and provides options (i.e., Actions) to the user to modify or remove a specified device type as well as the status and identifier of each device type chosen. Examples of device types shown include: Interactive Voice Response (IVR), Email, and Text Message (SMS). |

# Step-by-Step Instructions for User Logins Using MFA

These instructions demonstrate the login process for users who have MFA configured in their profile. Please follow each step listed below unless otherwise noted.

| **Step** | **Action** |
| --- | --- |
| **Step 1** | Go to <https://portal.cms.gov/>and select **Login to CMS Enterprise Portal**on the CMS Enterprise Portal.***Note:*** *The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari*.This picture displays the CMS Enterprise Portal login page and describes the first step in the login process for users who have MFA configured in their profiles.  |
| **Step 2** | Enter User ID and Password and select Login. Be sure to check the Agree box after you have read **and agreed to** the **Terms and Conditions** page. This picture displays the User ID and Password fields on the CMS Secure Portal login page and describes the second step in the process for users who have MFA configured in their profiles. Further, it provides instructions on completing the User ID and passwords fields as well as reading and agreeding to the Terms and Conditions. Enter user ID, passwrd and select the checkbox to agree to the Terms and Conditions. |
| **Step 3** | Select your authentication method from the drop down menu, then click send code This picture displays the "Select Authentication Method" drop-down menu on the CMS Secure Portal login page and describes the third step in the login process for users who have MFA configured in their profiles. Select your authentication method from the drop-down menu.This picture displays the "Text Message (SMS)" option and instructions on sending a security code to the users mobile device. Further, it describes the fourth step in the login process for users who have MFA configured in their profiles. Click the send code button and enter your security code. |
| **Step 4** | Enter your security code and select **verify to continue*****Note****: The ‘Security Code’ for the ‘e-mail’ and ‘One-Time Security Code’ options expires after 30 minutes. The ‘Security Code’ for the other MFA device types expires after 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.*This picture displays guidance on entering and verifing a security code and describes the fifth (and final) step in the login process for users who have MFA configured in their profiles. Enter your security code and select verfiy to continue.  |
|  **5** | Once you are successfully authenticated, your session will begin.This picture displays the cofirmation notice the user should receive upon successful authentication to the CMS Enterprise Portal.  |