

**CMS IDM  
MULTI-FACTOR  
AUTHENTICATION (MFA)  
DEVICE REGISTRATION**

## 1. 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's control can make this the least desirable option to receive a security code.*

## 2. 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.

The screenshot displays the 'My Profile' page. On the left is a navigation menu with options: View Profile, Change Profile, Change Business Contact Information, Change Password, Change Security Question, and Manage MFA Devices. The 'Manage MFA Devices' option is highlighted. The main content area is titled 'Manage Multi-Factor Authentication (MFA) Devices' and contains a table with one row of device information and a 'Register a Device' button.

Device Type	Identifier	Status	Actions
Email	martell66@gmail.com	Active	<a href="#">Edit</a>







[Register a Device](#)

**Step****Action**

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.

### My Profile

-  View Profile
-  Change Profile
-  Change Business Contact Information
-  Change Password
-  Change Security Question
-  Manage MFA Devices

#### Manage Multi-Factor Authentication (MFA) Devices

Device Type	Identifier	Status	Actions
 Email	martel066@gmail.com	Active	

#### Register Multi-Factor Authentication (MFA) Device

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 ID and Password.

Select the MFA device type that you want to use to login

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your MFA device within two attempts please log out, then log back in to try again.

Select MFA Device

- Text Message (SMS)
- Interactive Voice Response (IVR)
- Google Authenticator
- Okta Verify


**Step 2****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;

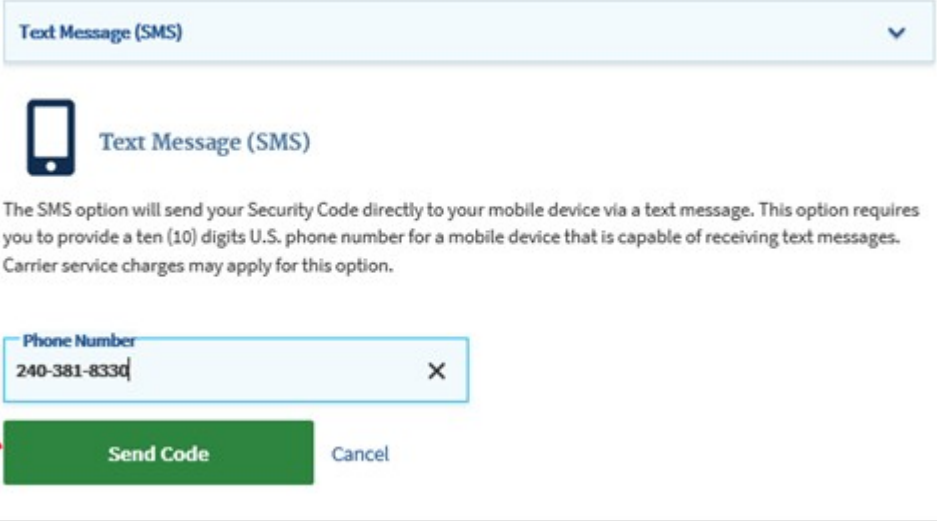
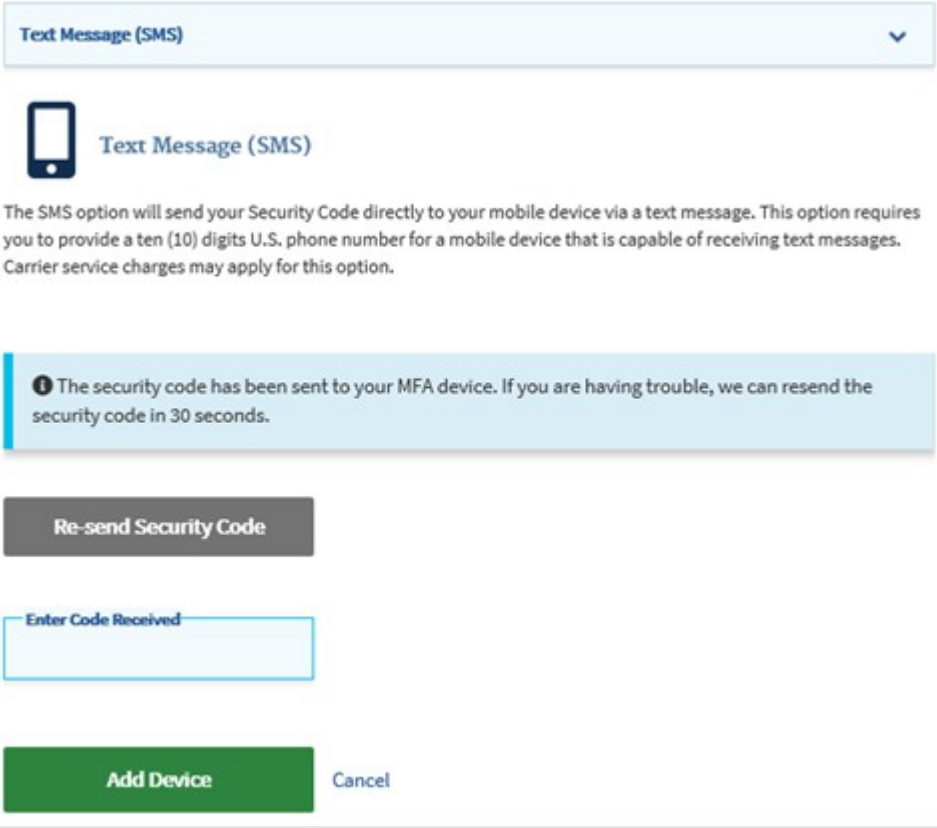
**. (period)** Creates a longer delay of approximately 5 seconds;

**\*(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	Action
Step 2a	<p><b>Using the Text Message (SMS)</b></p> <p>Follow these steps to use Text Message (SMS):</p> <ol style="list-style-type: none"> <li>Enter your phone number and select send code</li> </ol> 
Step 3	<p>Enter the security code received and select add Device...</p> 

Step

Action

After submitting the registration, a message will be displayed that you have successfully registered your device.



Confirmation

Changes to your profile have been successfully submitted.

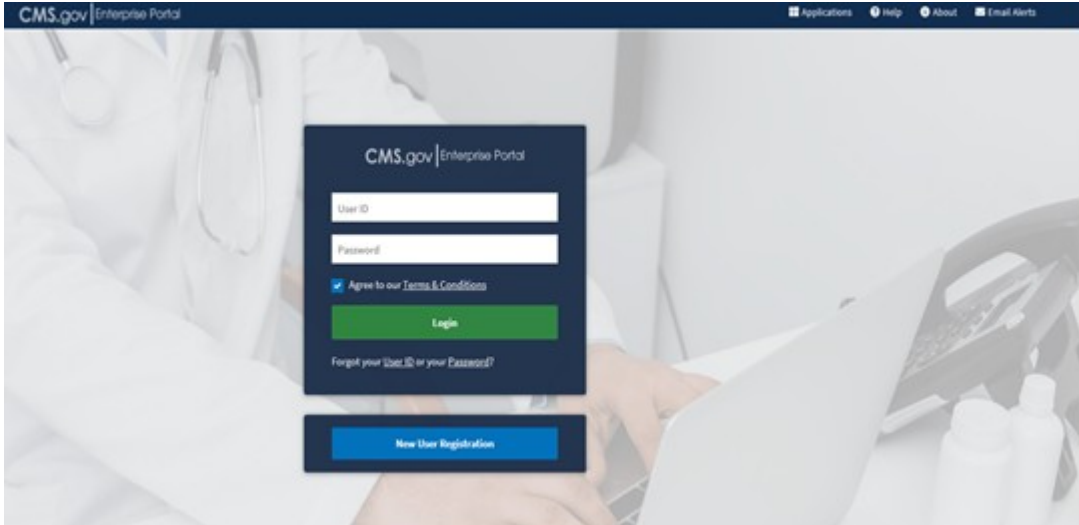
Device Type	Identifier	Status	Actions
 Interactive Voice Response (IVR)	+1 301-832-0884	Active	 Edit  Remove
 Email	martell66@gmail.com	Active	 Edit
 Text Message (SMS)	+1 240-381-8330	Active	 Edit  Remove

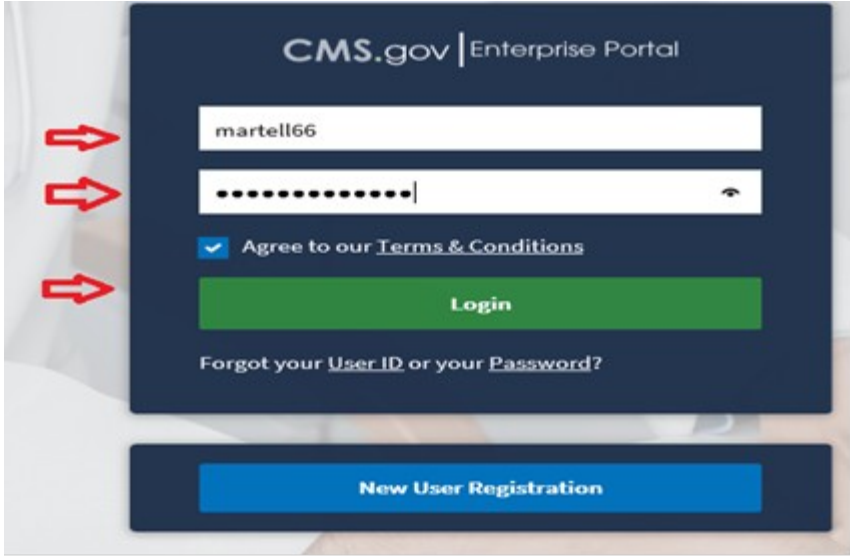
 Register a Device

Step 4

### 3. 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	<p>Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Enterprise Portal</b> on the CMS Enterprise Portal.</p> <p><b>Note:</b> <i>The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari.</i></p> 

Step	Action
Step 2	<p data-bbox="358 260 1382 327">Enter User ID and Password and select Login. Be sure to check the Agree box after you have read <b>and agreed to</b> the <b>Terms and Conditions</b> page.</p> 

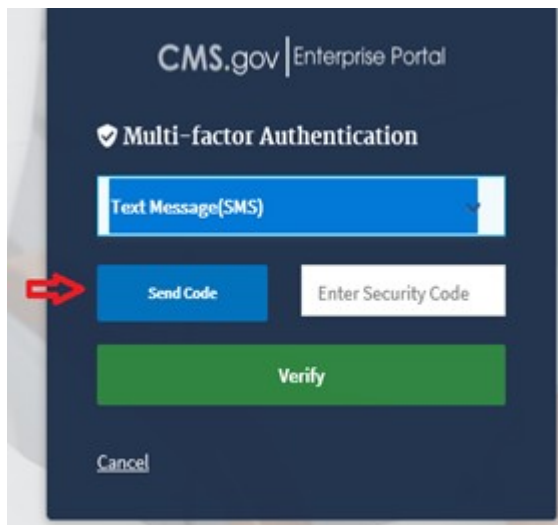


Step

Action

Select your authentication method from the drop down menu, then click send code

Step 3

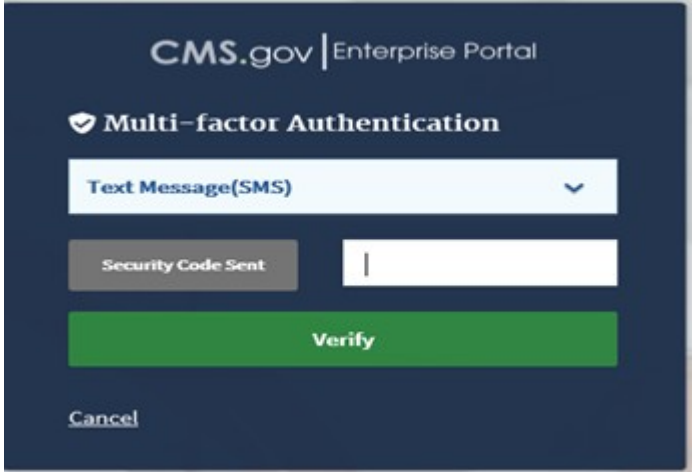


Step	Action
------	--------

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.



5

Once you are successfully authenticated, your session will begin.

