

Registering Multi-Factor Authentication (MFA) Devices

MFA is an additional security layer when logging into the CMS Enterprise Portal. MFA is required by CMS when accessing applications within IDM, and there are multiple MFA options. Additionally, when first time users log in, they are prompted to register at least one (1) MFA option, and additional MFA option(s) may be added/registered or edited at any time.

While registering your email address as an MFA device is a good idea, it's also the slowest option. There are several additional methods available in IDM that can provide the MFA code instantly and can be added to your account at any time.

MFA Options include:

- SMS (MFA code via text message) (Instant)
- Interactive Voice Response (IVR) (MFA code via phone call) (Instant)
- Google Authenticator (MFA code via browser extension or cell phone app) (Instant)
- Okta Verify (MFA code via cell phone app) (Instant)
- Email (MFA code via e-mail) (Slower)

To register an MFA Device, follow the steps below.

- 1. Go to the CMS Enterprise Portal (<u>portal.cms.gov</u>) or IDM (<u>https://home.idm.cms.gov/</u>) public home page and login with your User ID and password.
- 2. Select the down arrow icon showing next to your name at the top of page. Then select **My Profile** from the list to continue.

MS.gov My Enterprise Portal	• •	James Smith 🔻	🛛 Help	(+ Log Ou
My Portal	• •	y Profile		
	Previous Logi	no View Login History		
Welcome to CMS Enterprise Portal. Welcome James Smith to CMS Enterprise Portal. You've selected DEX (Data Exchange) System application during your registration. You can rev You may request access to other applications by selecting "Add Application" button.	quest access to this application by clicking here.			



3. The **My Profile** page displays. Select **Manage MFA Devices** in the left pane.

,	
	View Profile
View Profile	First Name:
Change Profile	Middle Name:
_	Last Name:
Change Business Contact Information	Date of Birth:
Change Password	Email Address:
Change Security Question and Answer	Phone Number:
Manage MFA Devices	Home Address Line 1:
	Home Address Line 2:
U Login History	City:
3 Markedo Dark Contact Information	1944 - C

4. Click on the **Register a device** button.

WS.gov My Enterprise Portal	III My Apps			James Smith 🔻	Help	C Log Ou
My Profile	Manage Multi-Factor	Authentication (1	MFA) Devices			
	Device Type	Identifier	Status	Actions		
View Profile	Text Message (SMS)	443-679-7512	Active			
Change Profile	8		Ed	Remove		
Change Business Contact Information	Register a device	-				
Change Password						
Change Security Question and Answer						
Manage MFA Devices						
Login History						

The registration section of the page displays.

MS.gov My Enterprise Portal	My Apps			James Smith	Help	œ
My Profile						
	Manage Multi-Factor	Authentication (1	MFA) Devices			
	Device Type	Identilier	Status	Actions		
View Profile	Text Message (SMS)	443-679-7512	Active	2 🖬		
Change Profile				Edit Remove		
Change Business Contac	ct information					
Change Password	Register Multi-Factor Adding a MFA Code to your login,	Authentication (MFA) Device Authentication (MFA), c	an make your login more secur		
Change Security Question	on and Answer Select the MFA device typ	e that you want to u	se to login			
Manage MFA Devices	Select MFA Device			~		
Login History						
My Help Desk Contact In	nformation					



- 5. Expand the Select MFA Device drop-down list to select one of the MFA Device Options below:
 - 1. Email (receive an email with the MFA code)
 - 2. SMS (receive a phone text messaging with the MFA code)
 - 3. Interactive Voice Response (receive a phone call with the MFA code)
 - 4. Google Authenticator (MFA code available via the browser extension or cell phone app)
 - 5. Okta Verify (receive a push notification through the cell phone app)

Device Type	Identifier	Status	Actions
Text Message (SMS)	443-679-7512	Active	Edit Remove
egister Multi-Factor ding a MFA Code to your login, providing an extra layer of pro	also known as Multi-Factor / tection to your User ID and F	MFA) Device Authentication (MFA Password.	ı), can make your login more secu
egister Multi-Factor ding a MFA Code to your login, providing an extra layer of pro lect the MFA device typ	t Authentication (1 also known as Multi-Factor / tection to your User ID and F pe that you want to us	MFA) Device Authentication (MF4 assword. se to login	.), can make your login more secu
egister Multi-Factor ding a MFA Code to your login, providing an extra layer of pro elect the MFA device typ elect MFA Device	t Authentication () also known as Multi-Factor r tection to your User ID and P oe that you want to us	MFA) Device Authentication (MFA Password. See to login	i), can make your login more secu
egister Multi-Factor ding a MFA Code to your login, providing an extra layer of pro elect the MFA device typ elect MFA Device relect MFA Device (IVFA Device Response (IVFA	t Authentication () also known as Multi-Factor , tection to your User ID and F pe that you want to us	MFA) Device Authentication (MF4 assword. as to login), can make your login more secu
egister Multi-Factor Iding a MFA Code to your login, providing an extra layer of pro elect the MFA device typ ielect MFA Device netractive Voice Response (IVF imail	t Authentication () also known as Multi-Factor , tection to your User ID and F be that you want to us	MFA) Device Authentication (MFA assword. ee to login), can make your login more secu

6. Follow the prompts to register the selected device and the message below will display upon successful completion of the registration.



Sample of an account with all MFA Devices added displayed below:

Manage Multi-Factor Authentication (MFA) Devices						
View Profile	Device Type	Identifier	Status	Actions		
Change Profile	Interactive Voice Response (IVR)		Active	Edit Remove		
Change Business Contact Information	Email		Active			
Change Password	Text Message (SMS)		Active	2		
Change Security Question and Answer	0			Edit Remove		
Manage MFA Devices	G ^{Google Authenticator}		Active	Remove		
1 Login History	Okta Verify			m		

For further assistance with MFA Devices contact the MAPD Help Desk via phone at 1-800-927-8069 or by email at <u>MAPDHelp@cms.hhs.gov</u>. The MAPD Help Desk hours of operation are Monday-Friday, 8:00 a.m. to 6:00 p.m. ET.