



# **Identity Management (IDM) System Instructions for Medicaid & CHIP Program (OneMAC) System Users**

October 2021

## Table of Contents

Table of Contents .....	ii
Overview .....	3
What is OneMAC? What is IDM? .....	3
Getting Started: Tips and Q&A .....	3
Getting Help .....	3
State IDM Role for OneMAC .....	4
Obtaining Access to OneMAC .....	5
Step 1: Register & Create an IDM Account .....	6
Step 2: Initiate Role Request for OneMAC Access .....	7
Step 3: Complete Remote Identity Proofing (RIDP) .....	9
Resolving RIDP Errors .....	10
If online identity proofing fails .....	10
If identity proofing via phone is successful .....	10
If identity proofing via phone fails .....	10
Step 4: Complete, Review & Submit Role Request .....	11
IDM Self-Service Account Features .....	12
Resetting a Forgotten Password .....	13
Unlocking a Locked Account .....	14
Recovering a Forgotten User ID .....	15
Changing an Expired Password .....	16
Managing User Account Profile Information .....	17
Accessing & Viewing a User Profile .....	17
Modifying Personal or Business Contact Information .....	18
Changing a Security Question & Answer .....	19
Changing the User Account Password .....	20
Managing MFA & Recovery Devices .....	21
Adding a Text Message (SMS) MFA & Recovery Device .....	22
Adding an Interactive Voice Response (IVR) MFA & Recovery Device .....	22
Adding an Okta Verify MFA Device .....	23
Adding a Google Authenticator MFA Device .....	23
Acronyms & Abbreviations .....	24
Glossary .....	25

## Overview

This document provides instructions for One Medicaid and CHIP (OneMAC) System users to obtain an Identity Management (IDM) System User ID and to request access to OneMAC. Additionally, this document describes how users can perform common tasks in IDM, such as resetting a forgotten password, unlocking a user account, and recovering a forgotten User ID.

**NOTE:** The images in this document were taken in training environment. The content in the images are reflective of test data, not production data.

## What is OneMAC? What is IDM?

OneMAC is a web-based system that allows the Centers for Medicare & Medicaid Services (CMS) and states to collaborate more effectively online in support of Medicaid and Children's Health Insurance Program (CHIP) initiatives, including serving as the administration and submission system for paper-based SPAs and 1915 waivers.

The IDM System provides the means for users to be approved to access many other CMS systems and applications. IDM governs access to CMS systems by managing the creation of user IDs and passwords, setting up multi-factor authentication (MFA), and the assignment of roles within CMS applications.

## Getting Started: Tips and Q&A

- **How do OneMAC and IDM work together from a user's perspective?** When users go to OneMAC at <https://onemac.cms.gov> and select "Login," an IDM sign-in screen will appear. After entering their IDM User ID and password, they will be logged in to OneMAC.
- **Can users select a link or a tile within IDM that would take them to OneMAC?** OneMAC can be accessed only directly via <https://onemac.cms.gov>. OneMAC cannot be accessed from within IDM.
- **What type of role or access should OneMAC users request in IDM?** State OneMAC users will request the following in IDM: (1) application access to OneMAC, and (2) the applicable IDM role for OneMAC.
  - All state users should request the *OneMAC State User role*
- **Where do users request roles like State Submitter or State System Administrator?** OneMAC-specific user roles must be requested directly in OneMAC at <https://onemac.cms.gov>.
- **Are OneMAC users required to use MFA or Recovery devices?** MFA is not required for OneMAC, but it may be required for other CMS system applications registered to a user's account. Additionally, all users are required to have a registered Recovery device, which can be used for IDM self-service account-access features. Users are highly encouraged to have multiple MFA and/or Recovery devices registered to their account.
- **When would users go directly to OneMAC vs directly to IDM?** Here are some additional examples:
  - Go to <https://onemac.cms.gov> to create, submit, and/or review State Plan Amendment (SPA) and Waiver related submission packages.
  - Go to <https://home.idm.cms.gov> to change a security question and answer, update personal or business contact information, or manage MFA and Recovery device information.

## Getting Help

The OneMAC help desk is available to assist from 9:00 AM to 5:00 PM Eastern Time, Monday through Friday. To contact the help desk:

- Call (833) 228-2540
- Email [OneMAC\\_HelpDesk@cms.hhs.gov](mailto:OneMAC_HelpDesk@cms.hhs.gov)

Please also contact the OneMAC help desk with any feedback, comments, and suggestions about this reference document and other OneMAC training and reference materials.

## State IDM Role for OneMAC

The table below displays a summary of the State IDM role for OneMAC, which users will request within IDM. The table also shows the role approval hierarchy.

IDM Role for OneMAC	Role Description	Role Request Approved By
OneMAC State User	U.S. State and Territories users. This role grants users access to the OneMAC application.	OneMAC Approver

## Obtaining Access to OneMAC

Below is an overview listing of the steps required for users to obtain access to OneMAC. Users will be able to sign in to OneMAC once the role request submitted in Step 4 is approved. Details on completing the below steps are available in the following subtopics of the same name.

- **Step 1:** Register & Create an IDM Account
- **Step 2:** Initiate Role Request for OneMAC Access
- **Step 3:** Complete Remote Identity Proofing (RIDP)
- **Step 4:** Complete, Review & Submit Role Request

## Step 1: Register & Create an IDM Account

If users already have an IDM User ID, they can skip to [Step 2: Initiate Role Request for OneMAC Access](#). Users can sign in to IDM immediately registering an account.

1. Select the **New User Registration** button on the IDM sign-in screen.

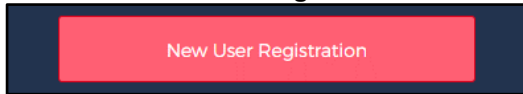


Figure 1: New User Registration button

2. Enter the personal and address information requested on the next two screens. Also select the **"I agree to the terms and conditions"** checkbox.

A form titled "Personal Information Screen" with fields for First Name, Middle Name (Optional), Last Name, Suffix (Optional) with a dropdown arrow, Date Of Birth (MM/DD/YYYY), E-mail Address, and Confirm E-mail Address. At the bottom, there is a "View Terms & Conditions" button and a checkbox labeled "I agree to the terms and conditions".

Figure 2: Personal Information Screen

A form titled "Address Information Screen" with a radio button selection for "US Address" (selected) or "Foreign Address". It includes fields for Home Address Line 1, Home Address Line 2 (Optional), City, State (dropdown), Zip Code, Zip Code Extension (Optional), and Phone Number. At the bottom, there are "Cancel", "Back", and "Next" buttons.

Figure 3: Address Information Screen

3. Enter a **User ID** and **password** and select a **security question** and an **answer**. Then select the **Submit** button.

A form titled "User ID, Passwords, Security Question Answer" with a progress indicator at the top showing three steps: Personal (1), Contact (2), and Credentials (3, active). The form includes fields for User ID, New Password, Confirm Password, Security Questions (dropdown), and Answer. At the bottom, there are "Cancel", "Back", and "Submit" buttons.

Figure 4: User ID, Passwords, Security Question Answer

## Step 2: Initiate Role Request for OneMAC Access

Users can sign in to IDM immediately after registering and creating an account. From that point, users will next request the applicable IDM role for OneMAC. For a description of all roles, refer to the [State IDM Role for OneMAC](#) topic.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **Role Request** tile.

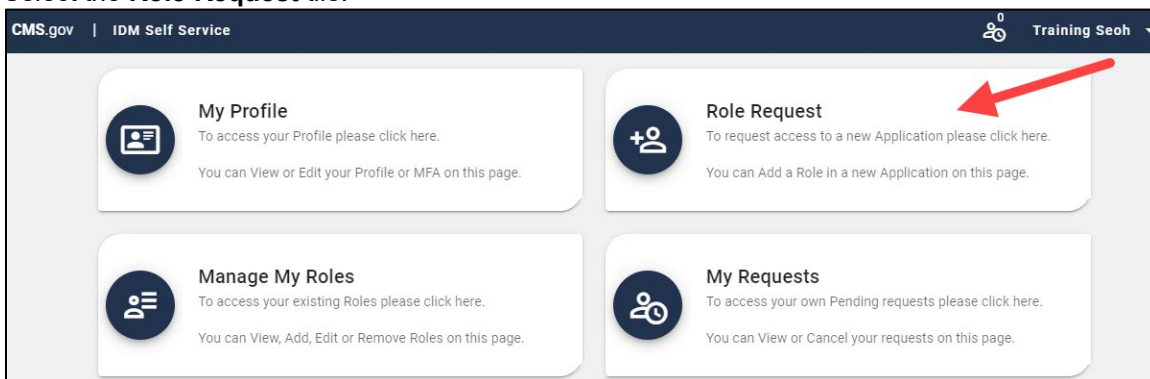


Figure 5: Role Request Tile

3. Select **OneMAC** from the **Select an Application** drop-down list.

The screenshot shows the 'Role Request' form. At the top, it says 'Role Request' and 'Optional fields are labeled as (Optional)'. Below this is a progress bar with three steps: 1. Application, 2. Role, and 3. Review. The 'Application' step is active. Below the progress bar is a dropdown menu labeled 'Select an Application'. The dropdown is open, showing a list of applications: MIDAS SAS Web, MLMS, Novitasphere, OneMAC, Open Payments, PRIS Plan Portal, PS&R/STAR, and QualityNet Service Center. A red arrow points to 'OneMAC'.

Figure 6: Select an Application drop-down list

4. Select the applicable role in the **Select a Role** drop-down list, as follows:
  - All **state users** must request the **OneMAC State User** role

Selected Application

OneMAC

One Medicaid and CHIP Program System (OneMAC) is a centralized portal that collects basic information from a state user on the state, SPA ID or waiver number, and requires certain documents to be uploaded for CMS review. The URL to access OneMAC is <https://onemac.cms.gov>.

View Helpdesk Details

Select a Role

End User

OneMAC CMS User

OneMAC State User

Approver

OneMAC Authorizer

Help Desk

OneMAC Helpdesk

Figure 7: Select a Role drop-down list



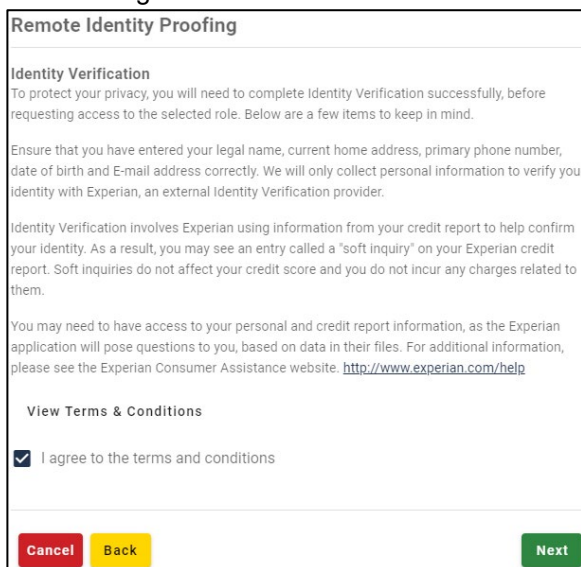
### Step 3: Complete Remote Identity Proofing (RIDP)

Remote Identity Proofing (RIDP) is a process that is used to verifying identity online. Most users will be required to complete RIDP (also known as identity verification) upon selecting a role to request in IDM (per the steps in the prior topic, “Step 2: Initiate Role Request for OneMAC Access”). If users are not prompted to complete RIDP, they can skip to the [Step 4: Complete, Review & Submit Role Request](#) topic.

#### NOTE:

- If online identity verification **completes successfully**, users will automatically be routed to a screen to select role attributes and to review and submit the role request. Instructions are in the [Step 4: Complete, Review & Submit Role Request](#) topic.
- If online identity verification **fails**, users should refer to the [Resolving RIDP Errors](#) topic for additional options.

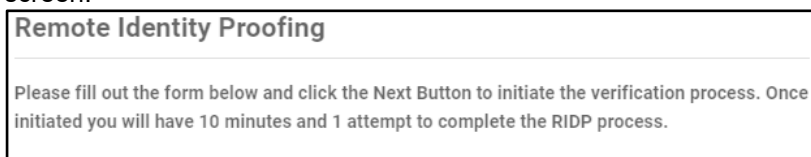
1. View and agree to the terms and conditions. Then select the **Next** button.



The screenshot shows a web form titled "Remote Identity Proofing". Below the title is a section "Identity Verification" with the following text: "To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind." It then provides instructions: "Ensure that you have entered your legal name, current home address, primary phone number, date of birth and E-mail address correctly. We will only collect personal information to verify your identity with Experian, an external Identity Verification provider." It also explains: "Identity Verification involves Experian using information from your credit report to help confirm your identity. As a result, you may see an entry called a 'soft inquiry' on your Experian credit report. Soft inquiries do not affect your credit score and you do not incur any charges related to them." A link is provided: "You may need to have access to your personal and credit report information, as the Experian application will pose questions to you, based on data in their files. For additional information, please see the Experian Consumer Assistance website: [http://www.experian.com/help](\"http://www.experian.com/help\")". Below this is a link "View Terms & Conditions". At the bottom, there is a checkbox labeled "I agree to the terms and conditions" which is checked. At the very bottom are three buttons: "Cancel" (red), "Back" (yellow), and "Next" (green).

Figure 8: Identity Verification screen

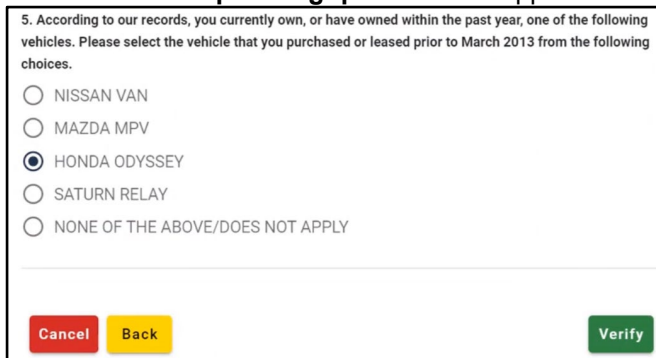
2. Complete the **Remote Identity Proofing** form. Then select the **Next** button in the lower-right corner of the screen.



The screenshot shows a web form titled "Remote Identity Proofing". Below the title is a text box with the following text: "Please fill out the form below and click the Next Button to initiate the verification process. Once initiated you will have 10 minutes and 1 attempt to complete the RIDP process." At the bottom right of the form is a green "Next" button.

Figure 9: Remote Identity Proofing form

3. Answer the **RIDP proofing questions** as applicable. Then select the **Verify** button.



The screenshot shows a web form titled "RIDP Proofing Questions". Below the title is a question: "5. According to our records, you currently own, or have owned within the past year, one of the following vehicles. Please select the vehicle that you purchased or leased prior to March 2013 from the following choices." Below the question are five radio button options: "NISSAN VAN", "MAZDA MPV", "HONDA ODYSSEY" (which is selected), "SATURN RELAY", and "NONE OF THE ABOVE/DOES NOT APPLY". At the bottom are three buttons: "Cancel" (red), "Back" (yellow), and "Verify" (green).

Figure 10: RIDP Proofing Questions

## Resolving RIDP Errors

If the Remote Identity Proofing (RIDP) identity verification process fails online, additional identity verification could be attempted via phone proofing, and, in some cases, manual proofing.

### If online identity proofing fails

1. Users should write down the **Review Reference Number** that appears in the error message on their screen (see below for an example of the error message).

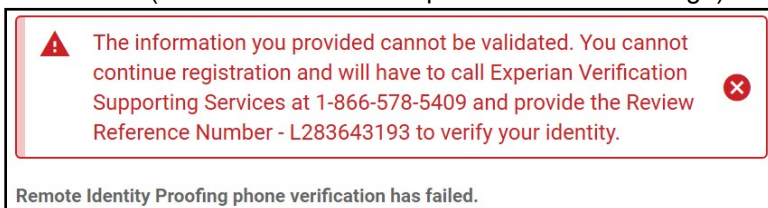


Figure 11: Remote Identity Proofing error

2. Select the **Cancel** button on the "Remote Identity Proofing" screen.
3. Select the **Confirm** button on the "Cancel Role Request Process" screen.
4. Call Experian Verification Support Services at 1-866-578-5409 for identity proofing via phone.

### If identity proofing via phone is successful

1. Re-initiate the role request in IDM (see the [Step 2: Initiate Role Request for OneMAC Access](#) topic for details).
2. Select the "I have already verified my identity with Experian" checkbox. Then select the **Next** button.

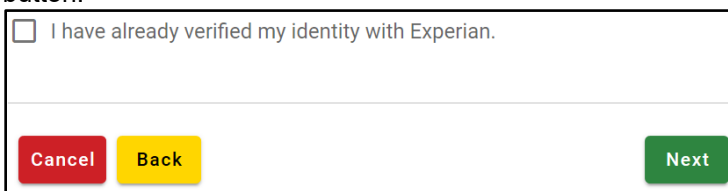


Figure 12: Identity Verification checkbox

3. Confirm the content on the Identity Information Verification screen is correct.
4. Select the **Next** button to continue with the role request process.

### If identity proofing via phone fails

1. Re-initiate the role request in IDM (see the [Step 2: Initiate Role Request for OneMAC Access](#) topic for details).
2. Select the **Try Again** button on the "The User data does not match the data from Experian" prompt.

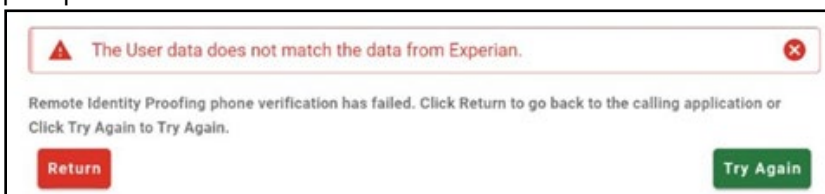


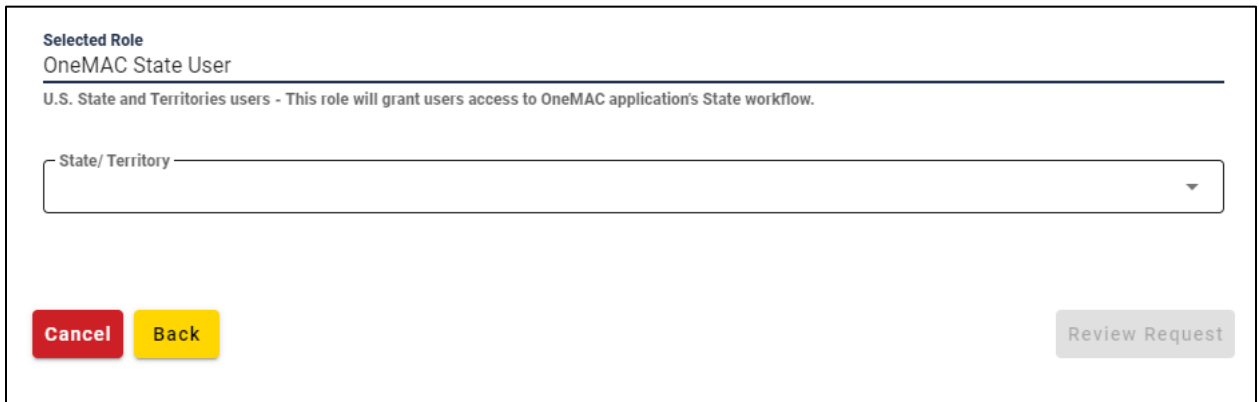
Figure 13: Identity Verification error

3. Review the content on the Identity Information Verification screen.
4. Select the **Next** button to continue the role request process.
5. If an error message appears again, take a screenshot of the entire screen (including the URL).
6. Select the **Return** button, and then cancel the role request.
7. Email the screenshot to the [OneMAC help desk](#) for manual identity proofing

## Step 4: Complete, Review & Submit Role Request

Upon successfully completing identity verification, users will be routed to the screens described below to complete, review, and submit the role request. Once the role request submitted in this step is approved, users will then be able to access OneMAC.

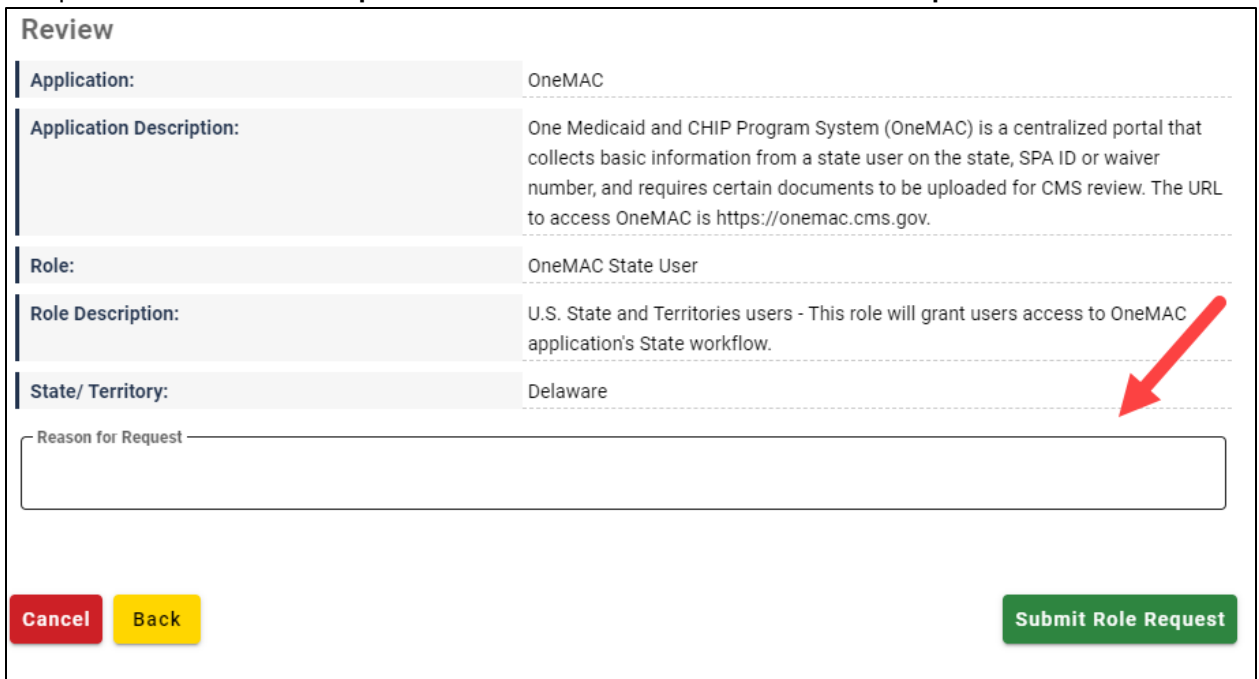
1. Select the applicable role attributes via the drop-down lists. Then select the **Review Request** button.



The screenshot shows a form titled "Selected Role" with the role "OneMAC State User". Below the role name is a description: "U.S. State and Territories users - This role will grant users access to OneMAC application's State workflow." There is a drop-down menu labeled "State/ Territory". At the bottom, there are three buttons: "Cancel" (red), "Back" (yellow), and "Review Request" (grey).

Figure 14: Role Attributes drop-down lists

2. Complete the **Reason for Request** text box. Then select the **Submit Role Request** button.



The screenshot shows a "Review" screen with a table of application details. The table has two columns: "Field" and "Value". The fields are "Application:", "Application Description:", "Role:", "Role Description:", and "State/ Territory:". The values are "OneMAC", "One Medicaid and CHIP Program System (OneMAC) is a centralized portal that collects basic information from a state user on the state, SPA ID or waiver number, and requires certain documents to be uploaded for CMS review. The URL to access OneMAC is <https://onemac.cms.gov>", "OneMAC State User", "U.S. State and Territories users - This role will grant users access to OneMAC application's State workflow.", and "Delaware". Below the table is a text box labeled "Reason for Request". At the bottom, there are three buttons: "Cancel" (red), "Back" (yellow), and "Submit Role Request" (green). A red arrow points to the "Reason for Request" text box.

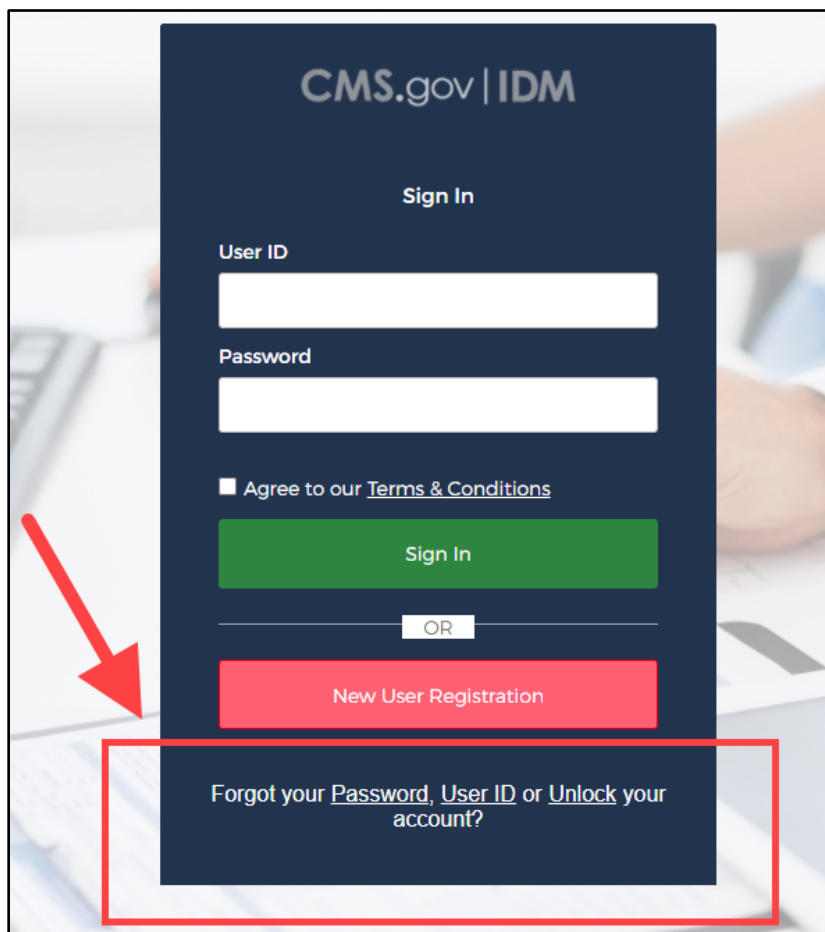
Figure 15: Text box for role request justification

## IDM Self-Service Account Features

IDM self-service features allows users to perform select account-access processes without requiring assistance from the OneMAC help desk. To use the self-service features, which are listed below, users must (1) remember their security question answer, and (2) have an active recovery device active their user profile.

- Resetting a forgotten password
- Recovering a forgotten User ID
- Unlocking a locked account
- Changing an expired password

Links to the self-service features for resetting a forgotten password, recovering a forgotten User ID, and unlocking an account are available via the respective Password, User ID, and Unlock links on the IDM sign-in screen (as shown below). Whereas the self-service feature for changing an expired password will automatically appear to users upon an attempt to sign in with an expired password.



CMS.gov | IDM

Sign In

User ID

Password

☐ Agree to our [Terms & Conditions](#)

Sign In

OR

New User Registration

Forgot your [Password](#), [User ID](#) or [Unlock your account](#)?

Figure 16: Self-service account-access links

## Resetting a Forgotten Password

Users can initiate the self-service reset forgotten password process via the Password link on the IDM sign-in screen.

**NOTE:** Users must remember their security question answer to complete this process.

1. Select the **Password** link on the IDM sign-in screen at <https://home.idm.cms.gov/>

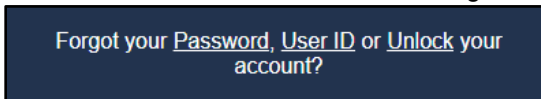


Figure 17: Self-Service Password link

2. Enter the **User ID** and select the applicable recovery method.

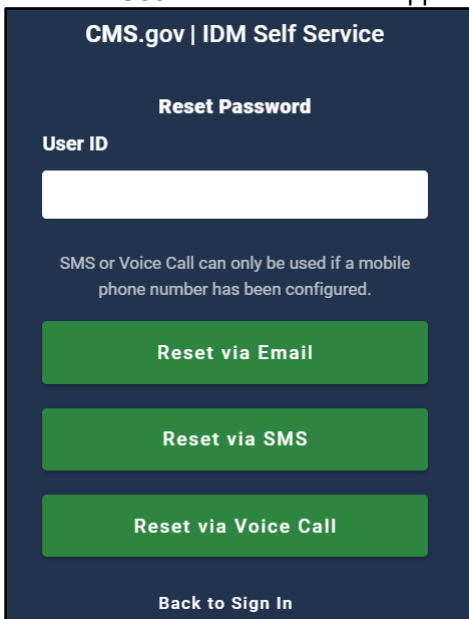
A dark blue form titled "CMS.gov | IDM Self Service" and "Reset Password". It contains a "User ID" label above a white input field. Below the field is a note: "SMS or Voice Call can only be used if a mobile phone number has been configured." There are three green buttons stacked vertically: "Reset via Email", "Reset via SMS", and "Reset via Voice Call". At the bottom is a link that says "Back to Sign In".

Figure 18: Reset Password screen

3. Select the **Reset Password** link in the "Forgot Password" email. Or, if applicable, enter the code provided via SMS text message or voice call.
4. Enter the applicable security question answer. Then select the **Reset Password** button.
5. Enter the new password in both the **New Password** field and the **Confirm Password** field. Then select the **Reset Password** button.

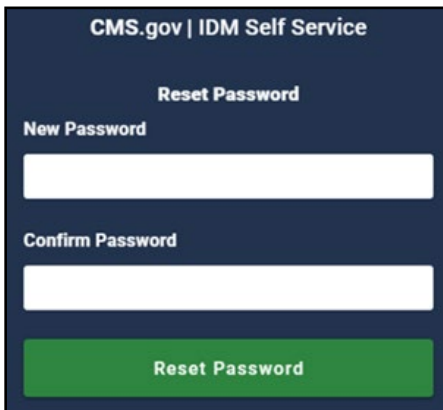
A dark blue form titled "CMS.gov | IDM Self Service" and "Reset Password". It contains two labels: "New Password" and "Confirm Password", each above a white input field. At the bottom is a green button labeled "Reset Password".

Figure 19: Password fields

## Unlocking a Locked Account

Users can initiate the self-service account unlock process by selecting the Unlock link on the IDM sign-in screen (as described in the below steps). Or, users can select the "Unlock Account" link in the "Account Unlock" email that is automatically sent to their email address upon their becoming locked.

**NOTE:** Users must remember their security question answer to complete this process.

1. Select the **Unlock** link on the IDM sign-in screen at <https://home.idm.cms.gov/>.

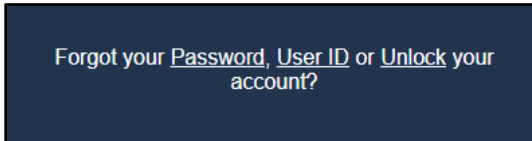


Figure 20: Self-service Unlock link

2. Enter a **User ID** and select the applicable recovery method.

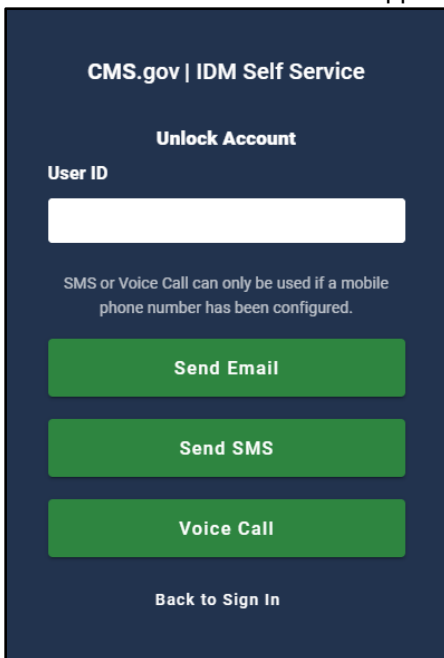
A dark blue form titled "CMS.gov | IDM Self Service" and "Unlock Account". It contains a "User ID" label above a white input field. Below the input field is a note: "SMS or Voice Call can only be used if a mobile phone number has been configured." There are three green buttons stacked vertically: "Send Email", "Send SMS", and "Voice Call". At the bottom is a link that says "Back to Sign In".

Figure 21: Unlock Account screen

3. Select the **Unlock Account** link in the "Account Unlock" email. Or, if applicable, enter the code provided via SMS text message or Voice Call.
4. Enter the applicable security question answer. Then select the **Unlock Account** button.

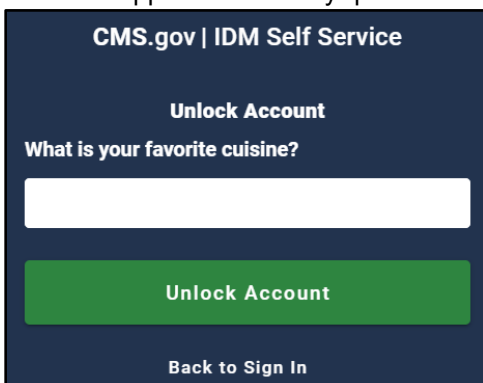
A dark blue form titled "CMS.gov | IDM Self Service" and "Unlock Account". It contains the question "What is your favorite cuisine?" above a white input field. Below the input field is a green button labeled "Unlock Account". At the bottom is a link that says "Back to Sign In".

Figure 22: Security question answer

## Recovering a Forgotten User ID

Users can initiate the self-service recover a forgotten User ID process by selecting the User ID link on the IDM sign-in screen.

1. Select the **User ID** link on IDM sign-in screen at <https://home.idm.cms.gov/>

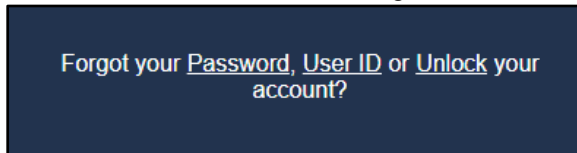
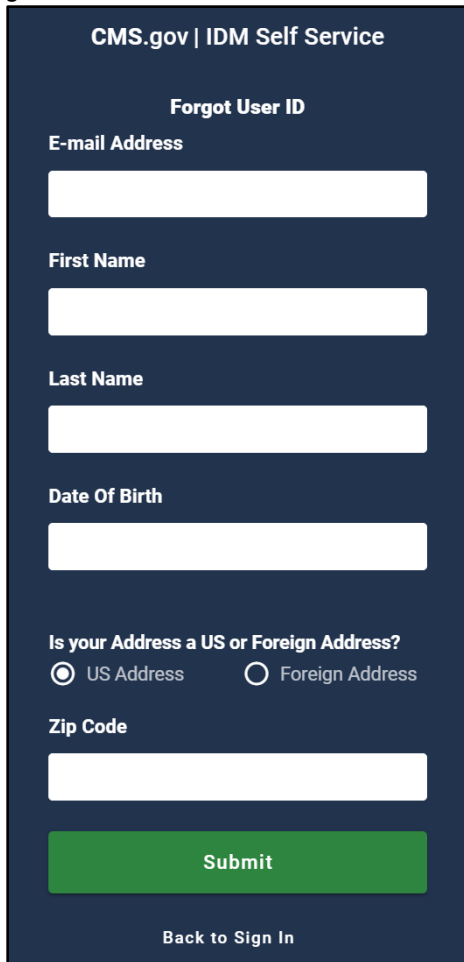


Figure 23: Self-service User ID link

2. Enter the requested information and select the **Submit** button. Then refer to the system-generated email for the recovered User ID.

A dark blue form titled "CMS.gov | IDM Self Service" and "Forgot User ID". It contains the following fields and options:

- E-mail Address**: A white text input field.
- First Name**: A white text input field.
- Last Name**: A white text input field.
- Date Of Birth**: A white text input field.
- Is your Address a US or Foreign Address?**: Two radio button options: "US Address" (selected) and "Foreign Address".
- Zip Code**: A white text input field.
- Submit**: A green button with white text.
- Back to Sign In**: A link at the bottom of the form.

Figure 24: Forgot User ID screen

## Changing an Expired Password

When users attempt to sign in to OneMAC or to IDM, if their password has expired, a “Your password has expired” message will appear.

1. Enter the expired password in the **Old Password** field.
2. Enter the new password in both the **New Password** field and the **Repeat Password** field.
3. Select the **Change Password** button.

The screenshot shows a dark blue background with the CMS.gov | IDM TEST logo at the top. Below the logo, the text "Your password has expired" is displayed. Underneath, a paragraph lists password requirements: at least 8 characters, a lowercase letter, an uppercase letter, a number, a symbol, no parts of the username, does not include the first or last name, and cannot be any of the last 24 passwords. At least 1 day(s) must have elapsed since the last password change. Below this text are three white input fields labeled "Old password", "New password", and "Repeat password". A green button labeled "Change Password" is positioned below the input fields. In the bottom right corner, there is a "Sign Out" link.

Figure 25: Expired Password screen



## Managing User Account Profile Information

Users can view and manage the following account information via the My Profile tile in IDM.

- View a summary of the user profile.
- View and modify personal and business contact information.
- Change account password and security question answer
- View and manage MFA and recovery devices

### Accessing & Viewing a User Profile

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile.

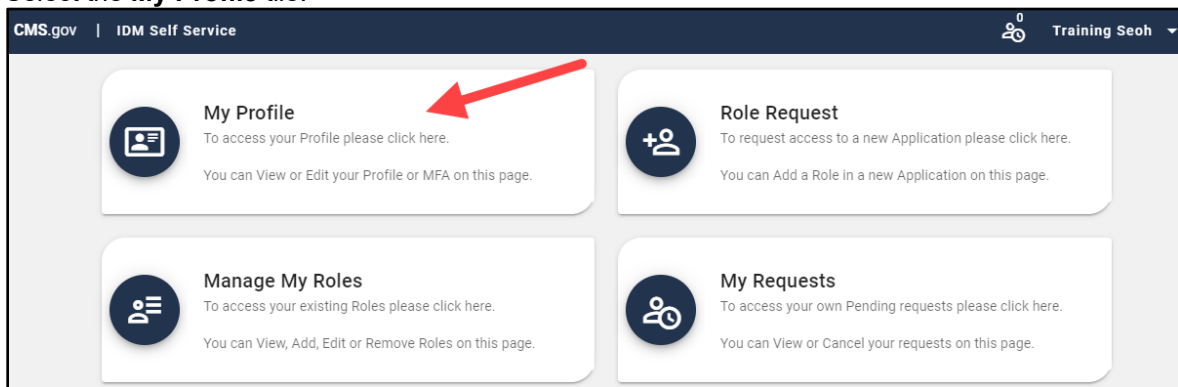


Figure 26: My Profile tile

3. A summary of the user profile appears on the My Information screen.

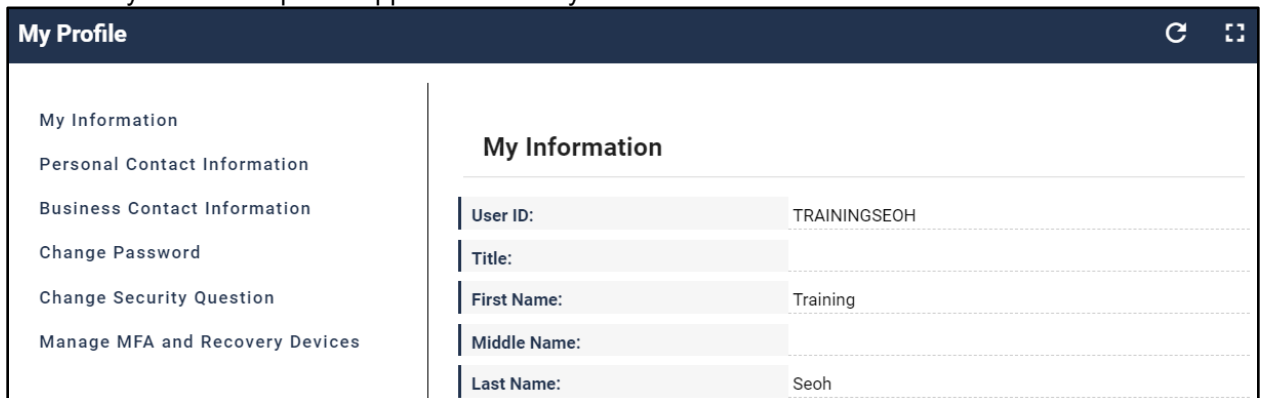


Figure 27: User Profile screen

## Modifying Personal or Business Contact Information

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile

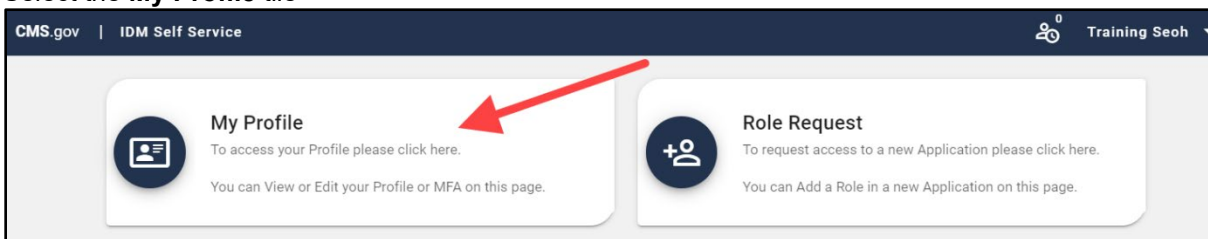


Figure 28: My Profile tile

3. Select the **Personal Contact Information** link or the **Business Contact Information** link, as applicable.

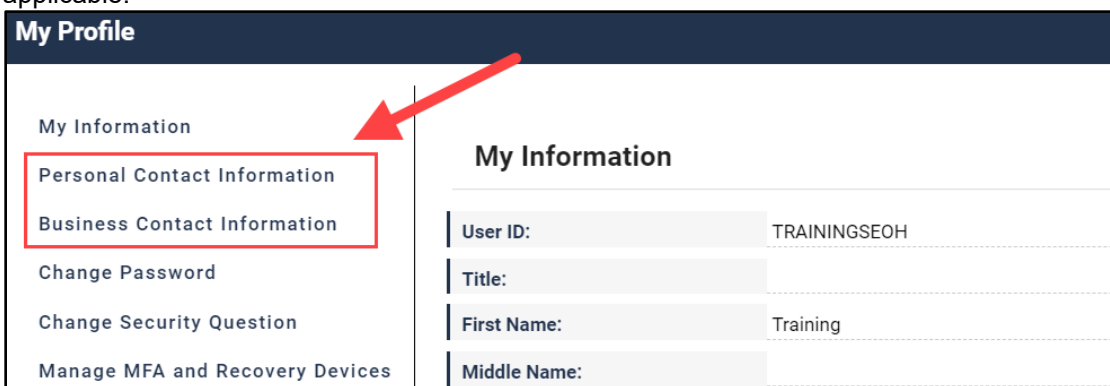


Figure 29: Contact Information links

4. Select the **Edit** button.

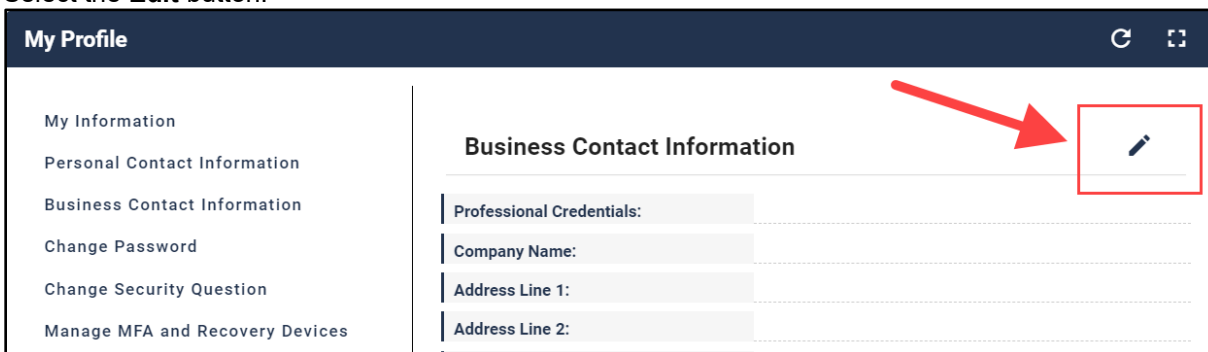


Figure 30: Edit button for Contact information

5. Update the modifiable fields as needed. Then select the **Submit Changes** button.

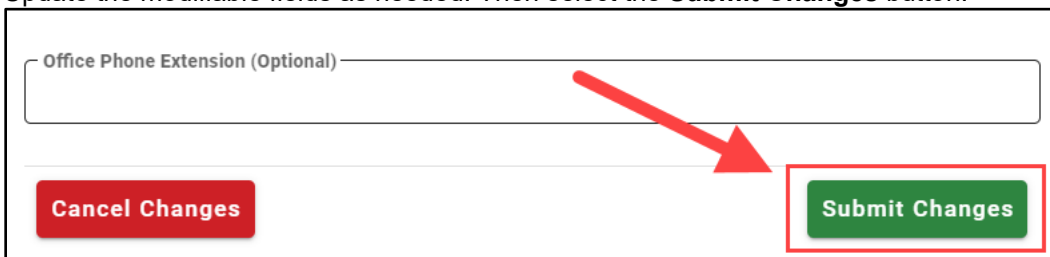


Figure 31: Submit Changes button

## Changing a Security Question & Answer

Users can change their security question and answer via the My Profile tile in IDM. Note that the security question answer must contain at least four characters, and it cannot contain parts of the user's first name, last name, password, or security question.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile.

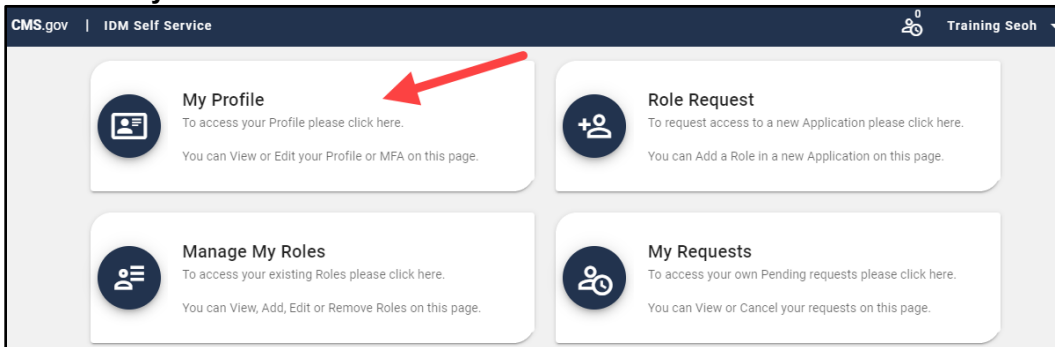


Figure 32: My Profile tile

3. Select the **Change Security Question** link.

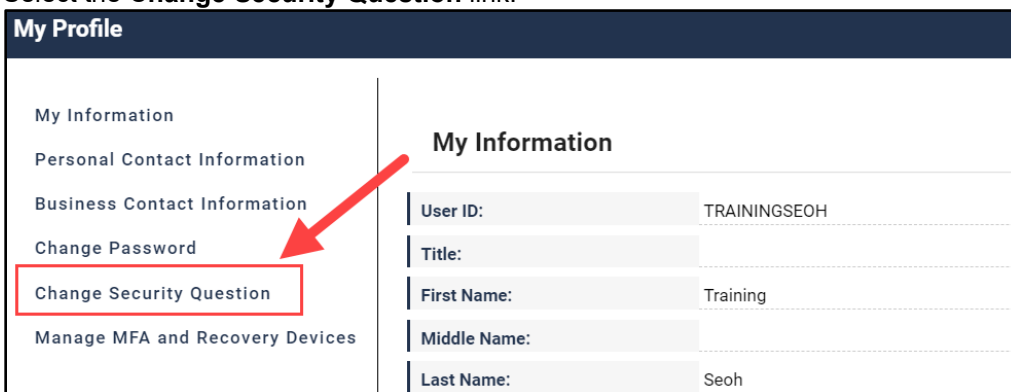


Figure 33: Change Security Question link

4. Select a question from the **Security Questions** drop-down list and enter the answer. Then enter the password and select the **Change Security Question** button.

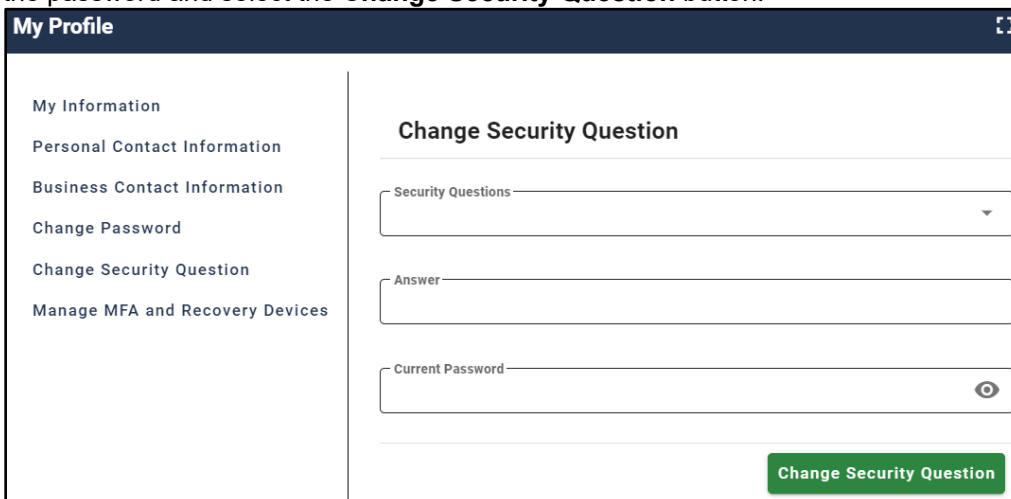


Figure 34: Change Security Question screen

## Changing the User Account Password

Users can change their IDM user account password via the My Profile tab in IDM, per the below steps. If users have forgotten their password and thus are unable to sign in to OneMAC or to IDM, refer to the [Resetting a Forgotten Password](#) topic for applicable instructions.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile.

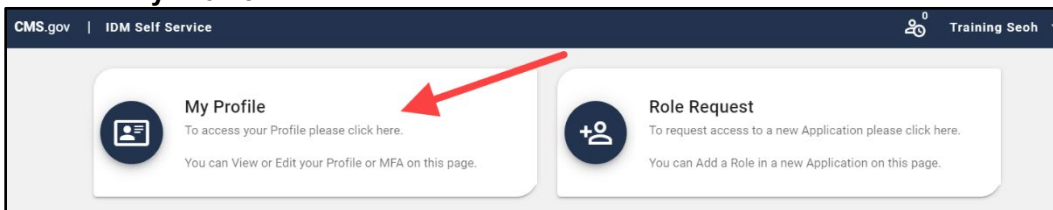


Figure 35: My Profile tile

3. Select the **Change Password** link.

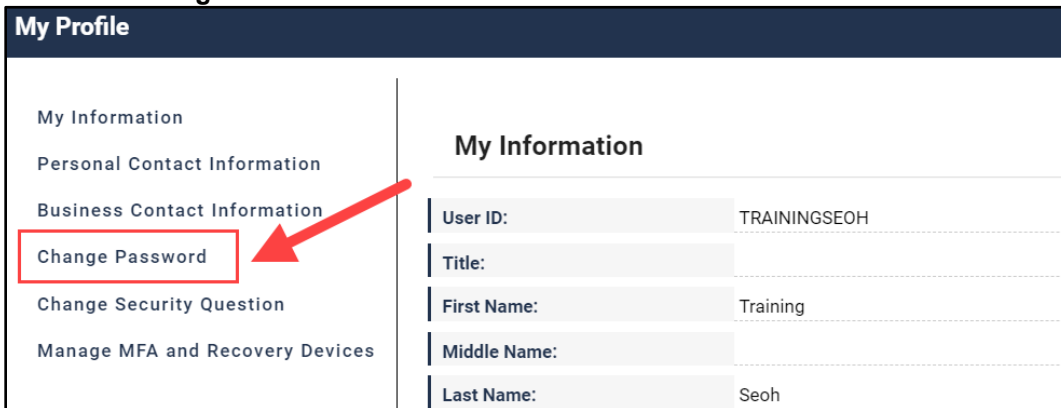


Figure 36: Change Password link

4. Enter the current and the new passwords in the applicable fields. Then select the **Change Password** button.

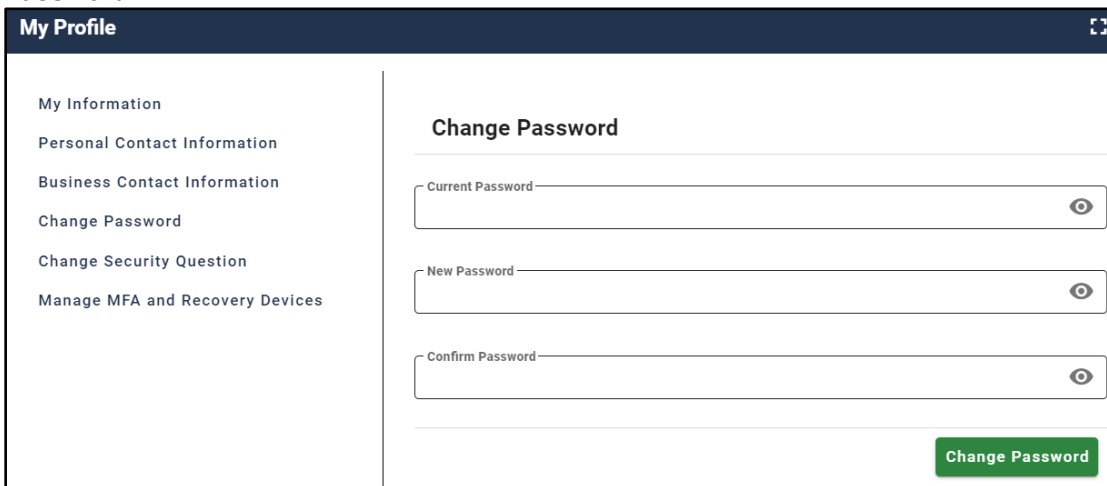


Figure 37: Change Password screen

## Managing MFA & Recovery Devices

Multi-factor authentication (MFA) is an optional additional layer of account security that functions essentially as a "second" password at sign-in. Email is automatically set as the default MFA device when activated.

Additionally, email is set as the default Recovery device for IDM user accounts. A Recovery device enables the use of IDM self-service account-access features such as resetting a forgotten password, unlocking an account, and recovering a forgotten User ID.

Below are the MFA and Recovery devices available for use with IDM.

- Email Address
- Interactive Voice Response (IVR)
- Text Message (SMS)
- Google Authenticator
- OKTA Verify

### IMPORTANT NOTES:

- Users are **highly** encouraged to have multiple MFA and/or Recovery methods enabled for their IDM account.
- MFA is not required for OneMAC; however, all users are required to have an active Recovery device, which can be used for IDM self-service account-access features.

**My Profile**

**Manage MFA and Recovery Devices**

The devices managed on this page are used for self-service password reset and self-service unlock account and apply to all users. The same devices are also used for Multi-Factor Authentication (MFA) logins but only apply to those users required to login with MFA for their role or application. Adding a device will not add MFA to your login if it is not already required for your role or application.

Type	Value	Status	Device Type	Actions
E-mail Address	macpro_helpdesk@cms.hhs.gov	Active	Recovery/MFA for Email	

[Add another device](#)

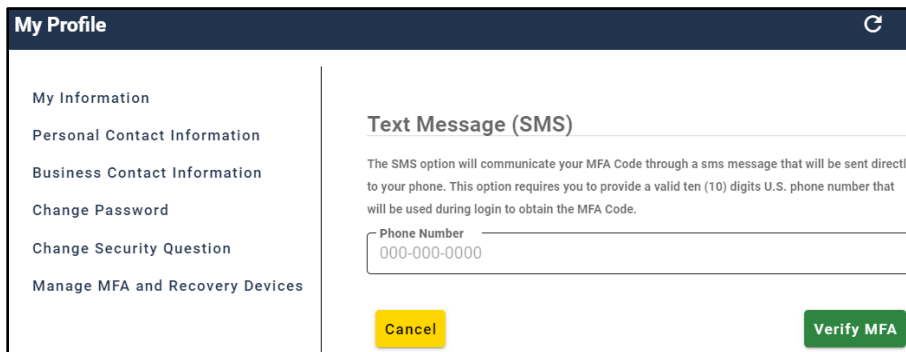
Adding a MFA Code to your login, also known as Multi-Factor Authentication (MFA), can make your login more secure by providing an extra layer of protection to your User ID and Password. Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your MFA device within two attempts please log out, then log back in to try again.

Figure 38: Manage MFA and Recovery Devices screen

## Adding a Text Message (SMS) MFA & Recovery Device

A text message (SMS) MFA and Recovery device delivers a one-time verification code via a text message that is sent directly to the phone number listed on the user's account.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile. Then select the **Manage MFA and Recovery Devices** link.
3. Select the **Text Message (SMS)** option in the **Add another device** drop-down list.
4. Enter the registered phone number. Then select the **Verify MFA** button.
5. Retrieve and enter the verification code.
6. Select the **Confirm MFA** button. A message will appear indicating the device was successfully added.



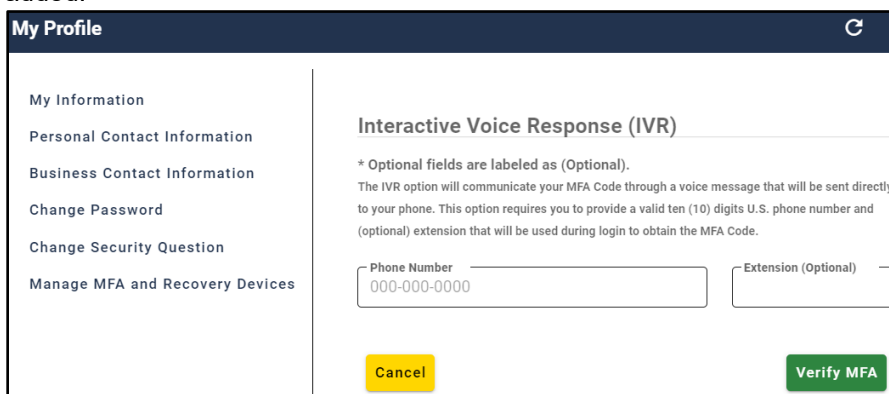
The screenshot shows the 'My Profile' page with a sidebar on the left containing links: My Information, Personal Contact Information, Business Contact Information, Change Password, Change Security Question, and Manage MFA and Recovery Devices. The main content area is titled 'Text Message (SMS)' and contains the following text: 'The SMS option will communicate your MFA Code through a sms message that will be sent directly to your phone. This option requires you to provide a valid ten (10) digits U.S. phone number that will be used during login to obtain the MFA Code.' Below this text is a 'Phone Number' input field with the placeholder '000-000-0000'. At the bottom of the form are two buttons: a yellow 'Cancel' button and a green 'Verify MFA' button.

Figure 39: Text Message (SMS) screen

## Adding an Interactive Voice Response (IVR) MFA & Recovery Device

An Interactive Voice Response (IVR) MFA and Recovery device delivers a one-time verification code via an automated voice message that is sent directly to the phone number listed on the user's account.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile. Then select the **Manage MFA and Recovery Devices** link.
3. Select the **Interactive Voice Response (IVR)** option in the **Add another device** drop-down list.
4. Enter the applicable phone number. Then select the **Verify MFA** button.
5. Retrieve and enter the verification code in the field provided.
6. Select the **Confirm MFA** button. A message will appear indicating the device was successfully added.



The screenshot shows the 'My Profile' page with the same sidebar as Figure 39. The main content area is titled 'Interactive Voice Response (IVR)' and contains the following text: '\* Optional fields are labeled as (Optional). The IVR option will communicate your MFA Code through a voice message that will be sent directly to your phone. This 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 MFA Code.' Below this text are two input fields: 'Phone Number' with placeholder '000-000-0000' and 'Extension (Optional)'. At the bottom of the form are two buttons: a yellow 'Cancel' button and a green 'Verify MFA' button.

Figure 40: Interactive Voice Response (IVR) screen

## Adding an Okta Verify MFA Device

The Okta Verify MFA device uses the Okta Verify mobile app to deliver a push notification to the user's smartphone or tablet mobile device.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile. Then select the **Manage MFA and Recovery Devices** link.
3. Select the **Okta Verify** option in the **Add another device** drop-down list.
4. Follow the on-screen prompts for installing and setting up Okta Verify.

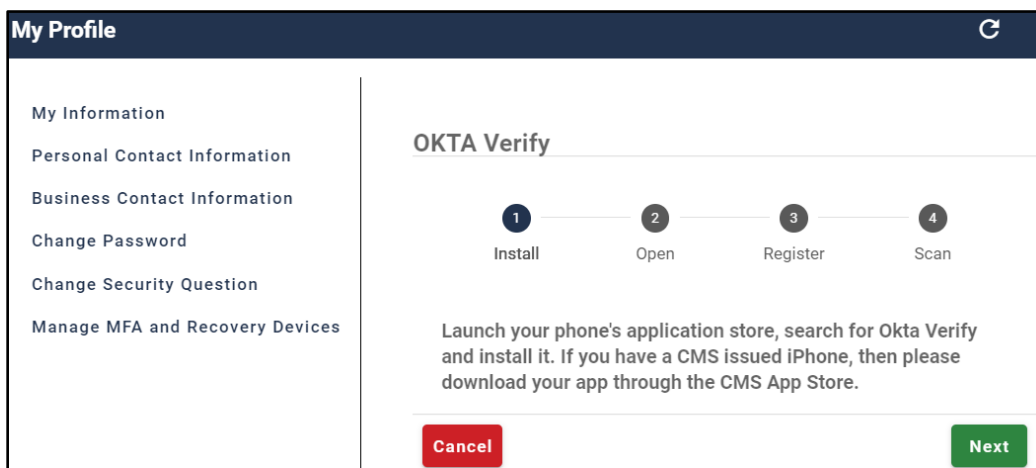


Figure 41: OKTA Verify screen

## Adding a Google Authenticator MFA Device

The Google Authenticator MFA device can use the Google Authenticator mobile app to deliver a one-time verification code to the user's smartphone or tablet mobile device. The Google Authenticator mobile app can receive MFA codes even in the absence of internet or mobile service connectivity.

1. Sign in to IDM at <https://home.idm.cms.gov/>
2. Select the **My Profile** tile. Then select the **Manage MFA and Recovery Devices** link.
3. Select the **Google Authenticator** option in the **Add another device** drop-down list.
4. Follow the on-screen prompts for installing and setting up Google Authenticator.

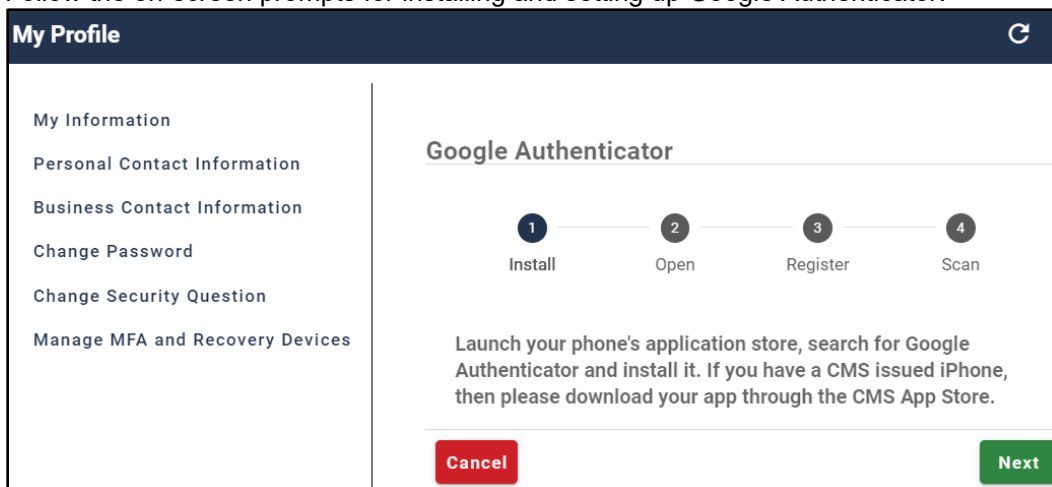


Figure 42: Google Authenticator screen

## Acronyms & Abbreviations

Term	Definition
CHIP	Children's Health Insurance Program
CMS	Centers for Medicare & Medicaid Services
IDM	Identity Management System
IVR	Interactive Voice Response
LOA	Level of Access
MFA	Multi-factor Authentication
OneMAC	One Medicaid and CHIP System
RD	Reference Document
RIDP	Remote Identity Proofing (also known as identity verification)
SMS	Short Message Service (also known as text messages)



## Glossary

Term	Definition
Role	A name, usually a function or title, given to a collection of access privileges or permissions within an application. A role defines what the user is allowed to do by virtue of having been assigned or granted that role. Each application defines the access privileges and permissions assigned to each role.
Role Attribute	A characteristic of a role that typically represents a functional limitation of the scope of a role's access privileges.
Security Question and Answer (SQA)	The security question is a question to which the user provides a unique answer. They both become part of the user's account and are used to authenticate the user when they access IDM's self-service functions.
Multi-factor Authentication (MFA)	MFA is an additional layer of security that functions as a "second" password. It is transmitted as a numeric code to the user's email (by default) or phone and is good for one sign in only.
Remote Identity Proofing (RIDP)	Describes the process that is used to confirm a person's identity. Most users will be required to complete RIDP as part of the process of being approved for a role in IDM. Users may have three opportunities to verify their identity. Verification occurs in the following order: <ul style="list-style-type: none"> <li>• Online Proofing - An identity verification procedure that uses Experian's computer-based Identity Verification service.</li> <li>• Phone Proofing - An identity proofing procedure that uses Experian's telephone-based Identity Verification service. Phone proofing is available only if a user's identity cannot be verified using online proofing.</li> <li>• Manual Proofing - An identity proofing procedure that is performed by an the OneMAC help desk. Manual proofing is an option only if the user is unable to first verify their identity through online proofing and phone proofing.</li> </ul>
Recovery	A process that allows a user to reset their own password or unlock their own account without the assistance of a help desk.
Recovery Device	An email, short message service (SMS), or interactive voice response (IVR) device such as a phone, that is used to authenticate a user during the recovery process.
OneMAC User Role	OneMAC-specific user roles that users will request and hold within OneMAC. These roles allow users to perform various functions within OneMAC. OneMAC user roles are separate from the roles that users request within IDM.
IDM Role for OneMAC	Roles that users request within IDM to obtain access to OneMAC.
IDM User ID	All OneMAC users are required to have an IDM User ID, which is used to access OneMAC and other CMS system applications.