Centers for Medicare & Medicaid Services

HETS Desktop (HDT)
Identity Management (IDM) System

User Guide

Version 1.5

3/10/2023

Document Number: USM-9003DD

Contract Number: HHSM-500-2017-00039I

Table of Contents

List of Figures

List of Tables

1. Introduction

This User Guide provides the information necessary for Clearinghouse and Direct Provider Submitters to effectively use the Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) Desktop (HDT) application.

1.1 HDT IDM User Guide Intended Audience

The intended audience of the HDT Identity Management (IDM) User Guide consists of the following users:

- New HDT users who create their user accounts via IDM.
- Existing HDT users who were migrated from the legacy Enterprise Identity Management system.

1.2 User Guide Purpose

Centers for Medicare & Medicaid Services (CMS) is dedicated to safeguarding Protected Health Information (PHI) and ensuring that only entitled Medicare providers and suppliers receive Medicare benefit information. CMS requires all Submitters to ensure that they are only sending active, valid Fee For Service (FFS) Medicare National Provider Identifier (NPI) numbers to the HETS 270/271 application.

Submitters must utilize the HDT application to register and maintain an updated record of their business relationships with their HETS 270/271 provider and/or supplier customers prior to submitting HETS 270/271 transactions. In addition, Submitters can verify if NPI numbers are eligible for use with the HETS 270/271 application.

This user guide describes the IDM Self-Service User Interface (UI) and the HDT application.

This user guide provides users with step-by-step instructions for performing the following tasks (based on access privileges) using the IDM Self-Service UI:

- How to access the IDM System
- How to register a new IDM user account
- How to sign in to the IDM System
- How to use the IDM My Profile function
- How to use the IDM Manage My Roles function
- How to use the IDM My Requests function
- How to request HDT access via IDM
- How to set up Remote Identity Proofing (RIDP)
- How to unlock an IDM account
- How to reset expired or forgotten passwords
- How to view and manage user profile settings
- How to manage requests that are pending action by an approver
- How to use the HDT application to create Submitter ID/Provider relationships

- How to use the HDT application to check the status of a Submitter ID/Provider relationship
- How HETS clearinghouse submitters use batch functionality to perform mass updates of Submitter ID/NPI relationships

This user guide provides users with step-by-step instructions for performing the following tasks using the HDT application:

- NPI management via the HDT UI including querying, adding, or terminating Submitter ID/NPI relationships
- NPI management via the HDT NPI Batch Management including querying, adding, or terminating Submitter ID/NPI relationships
- Troubleshooting common HDT errors

1.3 Identity Management (IDM) System Overview

CMS created the IDM System to provide Business Partners with a means to request and obtain a single User ID which they can use to access one or more CMS applications, including HDT. The IDM System uses a cloud-based distributed architecture that supports the needs of CMS applications while providing an improved user experience on desktop and laptop computers as well as tablet and smartphone mobile devices.

1.4 HDT Application Overview

Users access the HDT application after authenticating their identity using an IDM User ID and password. Approved IDM Users must add the HDT role to their IDM profile via the IDM UI then obtain CMS approval before HDT access will be granted.

The HDT application is used by Submitters to:

- Register their HETS 270/271 provider/supplier customers with CMS to establish an NPI/Submitter relationship
- Maintain a list of all NPIs that their organization will be sending to the HETS 270/271 application
- Query the status for one or more NPIs via the HDT application
- Review their current Submitter profile

The HDT application will validate NPIs that are either being queried or added by the Submitter to ensure that they are valid FFS Medicare providers or suppliers. Additionally, HDT will check the status of an NPI with Medicare daily. If an NPI is deemed to be invalid by Medicare, the NPI will also be invalid in HDT and will be prohibited from receiving PHI from the HETS 270/271 application.

In addition to validating that the NPIs submitted to the HETS 270/271 application are active and valid with Medicare, the HDT application will validate that there is a known Submitter/Provider relationship between the HETS 270/271 Submitter and the FFS Medicare provider or supplier.

The HDT application is integrated with the HETS 270/271 application. The NPIs submitted on 270 eligibility requests will be validated in real-time. If a Submitter sends an eligibility request with an NPI number that is a) not on file with CMS, b) not an active, valid FFS Medicare Provider at the time the request is processed, or c) not found as associated with the Submitter, then a 271 AAA error (with an appropriate error code) will be returned instead of entitlement information. Refer to Section 8.3 of the *HETS 270/271 Companion Guide* for more information on the 271 AAA error codes.

The HDT application allows for both manual and batch NPI management processes. The manual NPI management options allow Clearinghouse and Direct Provider Submitters to query, add, and terminate their relationships with providers and/or suppliers one NPI at a time. The screen displays the session’s most current 25 responses in order, with the most recent response listed first.

The batch NPI management option allows Clearinghouse Submitters to query, add, and terminate their relationships for multiple NPIs at one time. The NPIs must be submitted in a flat text file that can be uploaded via the HDT application. HDT Clearinghouse Submitter Users can upload batch files and then receive response files back via the HDT application. HDT batch input files are stored in the User’s HDT history for 60 days before they are archived; HDT batch output files are stored in the User’s HDT history for at least 120 days before they are archived.

2. Referenced Documents

The *HETS 270/271 Companion Guide* provides information related to the HETS 270/271 application described throughout this document. Users can obtain the latest version of the *HETS 270/271 Companion Guide* in the Downloads section at the following website link:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index

If problems and/or questions arise while accessing the HDT application, contact the Medicare Customer Assistance Regarding Eligibility (MCARE) Help Desk at 1-866-324-7315 or at MCARE@cms.hhs.gov Monday through Friday, from 7:00 AM to 7:00 PM ET.

3. Quick Reference Guide

Table 1: Quick Reference Guide

Questions	Answers
Need to sign-in to HDT?	See Section *14.1 – Log In to the HDT Application*
Need to log in with existing credentials?	See Section *7 – How to Sign In to the IDM System*
Need to add an HDT role to an existing account?	See Section *12 – How to Request HDT Access Via IDM*
Need to add a Multi-factor Authentication (MFA) device to your IDM account?	See Section *9.8 – How to Manage IDM MFA Devices*
Has your password been reset?	See Section *7.1.1 – The User's Password*
Need to change your password?	See Section *9.6 - How to Change the IDM User Account Password*
Need to create an entirely new IDM account?	See Section *6 – How to Register a New IDM User Account*
Need to add a Multi-factor Authentication (MFA) device to your IDM account?	See Section *9.8 – How to Manage IDM MFA Devices*

4. Prepare to Access the HDT Application via IDM

Users who access HDT using IDM with a desktop or laptop computer may need to perform software updates or configure web browser settings and privacy settings. Users who access HDT using IDM via a mobile computing device such as a smartphone or tablet generally have less control over updates and privacy settings. Therefore, the procedures discussed in this section may not apply to mobile device users.

4.1 Verify Web Browser Support

The HDT application and IDM were tested for compatibility with current versions of the following modern web browsers:

- Microsoft Edge (Legacy) [1, 2]
- Google Chrome
- Mozilla Firefox
- Safari

All the web browsers listed above are configured by default to receive regular security updates and patches. Even in cases where the user's organization manages operating system and application software updates, users who access HDT via IDM with one of these web browsers should not encounter compatibility issues.

4.2 Verify Screen Resolution

The HDT application and IDM are optimally viewed on a display resolution of 1366 x 768. All images that are displayed on modern computing devices are composed of a matrix of thousands of tiny dots called pixels. This matrix is generally expressed as width times height (example: 1366 pixels wide x 768 pixels high or 1366 x 768). A device's screen resolution therefore refers to the size of this matrix. The more pixels the screen can display, the higher the resolution, and the better on-screen text and images will look. The default display resolution setting for modern desktop, laptop, and mobile computing devices generally equals or exceeds 1366 x 768. The HDT application and IDM support older devices with a minimum resolution of 800 x 600.

Note: Modern desktop and laptop computers configure Windows 8, Windows 10, and MacOS X operating systems to a display resolution that meets or exceeds 1366 x 768. Users of older devices may need to change their display resolution settings if the current setting does not display the IDM System UI properly.

Note: Modern desktop and laptop computers configure Windows 8, Windows 10, and MacOS X operating systems to a display resolution that meets or exceeds 1366 x 768. Users of older devices may need to change their display resolution settings if the current setting does not display the IDM System UI properly.

[1] Microsoft Edge (Legacy) is the default web browser on Windows 10 PCs. Many enterprise users still have this as their default web browser.

[2] The New Microsoft Edge was released on January 15, 2020. Some non-enterprise users have received automated installations of the New Edge browser as part of a Windows 10 update.

4.3 Cautions and Warnings

Web browser capabilities such as back, forward, refresh, and logging out should not be used during HDT application sessions.

Users should manually enter all internet addresses (Uniform Resource Locators, or URLs) into the internet browsers. CMS discourages Users from utilizing browser bookmarks with the HDT application.

To optimize access to the HDT application, please disable pop-up blockers prior to use.

CMS discourages HDT Users from utilizing Autofill or Auto-populate features of internet browsers. Users should disable these features in their browsers when using HDT.

HDT Users should adjust their internet browser settings to prevent caching when using HDT. Web browsers with large cache settings can store web pages on the user’s computer for extended periods of time. Because the HDT application framework has been developed to use similar page components, it is important that the user’s browser is set to ensure that it tries to locate and retrieve a fresh instance of the HDT page and the data content.

HDT Users should enable JavaScript and adjust any zoom features to ensure that they are not seeing the screen in too wide of a view.

HDT Users should disable Compatibility View settings in their internet browsers to ensure proper display of the HDT pages.

5. Description of Key HDT User Authentication Mechanisms

The HDT application uses IDM to confirm the User’s account credentials. HDT uses the following security mechanisms:

- HDT User ID policy
- HDT password policy
- Multi-factor Authentication (MFA)
- User uniqueness checks

5.1 HDT User ID Policy

The HDT User ID policy combines application specific guidelines and CMS password policy. IDM User IDs that are used to access HDT must conform to the following guidelines:

- Only personnel from HETS Clearinghouse and Direct Provider Submitters will be granted permission to access the HDT application. Users must be associated with an organization that has an active, valid HETS 270/271 Submitter ID.
- HDT Users must have an IDM User ID that is 32 characters or less to utilize the HDT application.
- The HDT application allows the IDM User ID and IDM User first and last names to contain certain special characters. Special characters apostrophe (‘ ‘ ‘), hyphen (‘ - ’) and spaces are compatible with HDT in the User ID and first and/or last name. Period (‘ . ‘) and underscore (‘ _ ‘) are also permitted in the User ID. The at sign (‘ @ ‘) is permitted as part of the User ID, but only when used as part of an email address format.

Users who request the HDT role for an existing IDM User ID that is greater than 32 characters and/or have a User ID or User first or last name that contains any special characters outside of the allowable situations noted above will not be granted access to the HDT application.

5.2 HDT Password Policy

The HDT password policy combines application specific guidelines and CMS password policy. Passwords that are used to access HDT must conform to the following guidelines:

- They must be at least 15 characters in length.
- They must contain one uppercase letter, one lowercase letter, and one number.
- Special characters are optional for use in the password. If used, the following special characters are acceptable: “ ! # $ % & ‘ ( ) * + , - . / \ : ; < = > ? @ [ ] ^ _ ` { | } ~.
- They must NOT contain a space.
- They must NOT contain parts of the user’s First Name, Last Name, or User ID.
- They must be different than the last six passwords used.
- 24 hours must have elapsed since the last password change.

5.3 Multi-Factor Authentication

Email is automatically set up as the default Multi-Factor Authentication (MFA) factor for all users that are required to sign in with MFA. MFA users may use the My Profile function to register additional MFA factors after they sign in. In addition to email, the IDM System supports the following MFA factors:

- Interactive Voice Response (IVR)
- Google Authenticator (Chrome browser plug-in and mobile app)
- Okta Verify
- Short Message Service (SMS) Text Message

Some MFA factors are also used to authorize Self-Service functions. Table 2: Summary of MFA Factors and Their Functions provides a summary of these functions. [3]

Table 2: Summary of MFA Factors and Their Functions

MFA Factor	Self-Service Password Reset	Self-Service Account Unlock	MFA
Email	Yes	Yes	Yes
SMS	Yes	Yes	Yes
IVR	Yes	Yes	Yes
Google Authenticator	No	No	Yes
Okta Verify	No	No	Yes

Note: The procedures described in this user guide will use the Email MFA factor when describing login procedures, self-service password reset procedures, and self-service account unlock procedures.

5.4 User Uniqueness Checks

CMS security policy requires that each user be uniquely identified. When a user creates an account, the information they submit is subjected to two uniqueness checks. The purpose of these checks is to maintain the integrity of the user information that is used by the IDM System for user authentication. The following uniqueness checks are conducted:

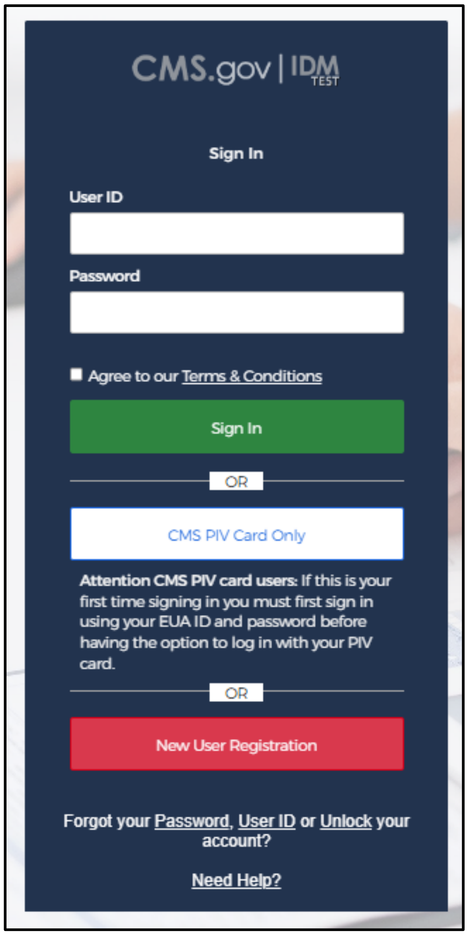
- The combination of the submitted first name + last name + email address must be unique.
- The submitted Social Security Number (SSN) must be unique.

[3] Some elements of the IDM Self-Service UI use the term MFA device. For the purpose of this user guide, MFA device and MFA factor are synonymous.

6. How to Register a New IDM User Account

This section provides the steps that users must follow to register a new user account on the IDM System.

1. Navigate to https://home.idm.cms.gov/.

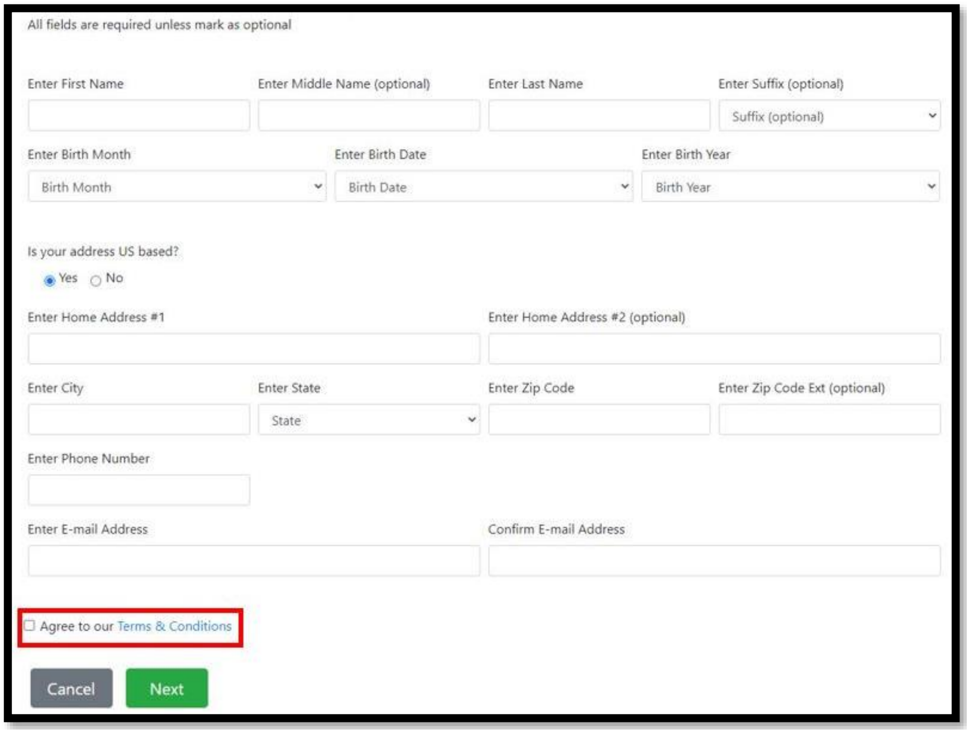


Attention CMS PIV card users: If this is your first time signing in you must first sign in using your EUA ID and password before having the option to log in with your PIV card.

Forgot your Password, User ID or Unlock your account?

Figure 1: IDM System (New User Registration Button Highlighted)

2. Click the Registration button.



All fields are required unless mark as optional

Enter First Name | Enter Middle Name (optional) | Enter Last Name | Enter Suffix (optional): Suffix (optional)

Enter Birth Month: Birth Month | Enter Birth Date: Birth Date | Enter Birth Year: Birth Year

Is your address US based?

● Yes ○ No

Enter Home Address #1 | Enter Home Address #2 (optional)

Enter City | Enter State: State | Enter Zip Code | Enter Zip Code Ext (optional)

Enter Phone Number

Enter E-mail Address | Confirm E-mail Address

□ Agree to our Terms & Conditions

Figure 2: IDM System User Registration Form

3. Enter the Name and Birth Month, Birth Date, and Birth Year information into the respective fields of the IDM System User Registration form.

4. If the home address is located inside the US, keep the default "US Address" setting. If the home address is located outside of the United States, click the "Foreign Address" radio button. [4]

5. Enter the Home Address, Phone Number, and Email Address information into the respective fields. [5, 6, 7, 8]

6. Click the Terms & Conditions link, read the IDM System terms and conditions, click the checkbox to acknowledge agreement with the Terms and Conditions, then click the Next button.

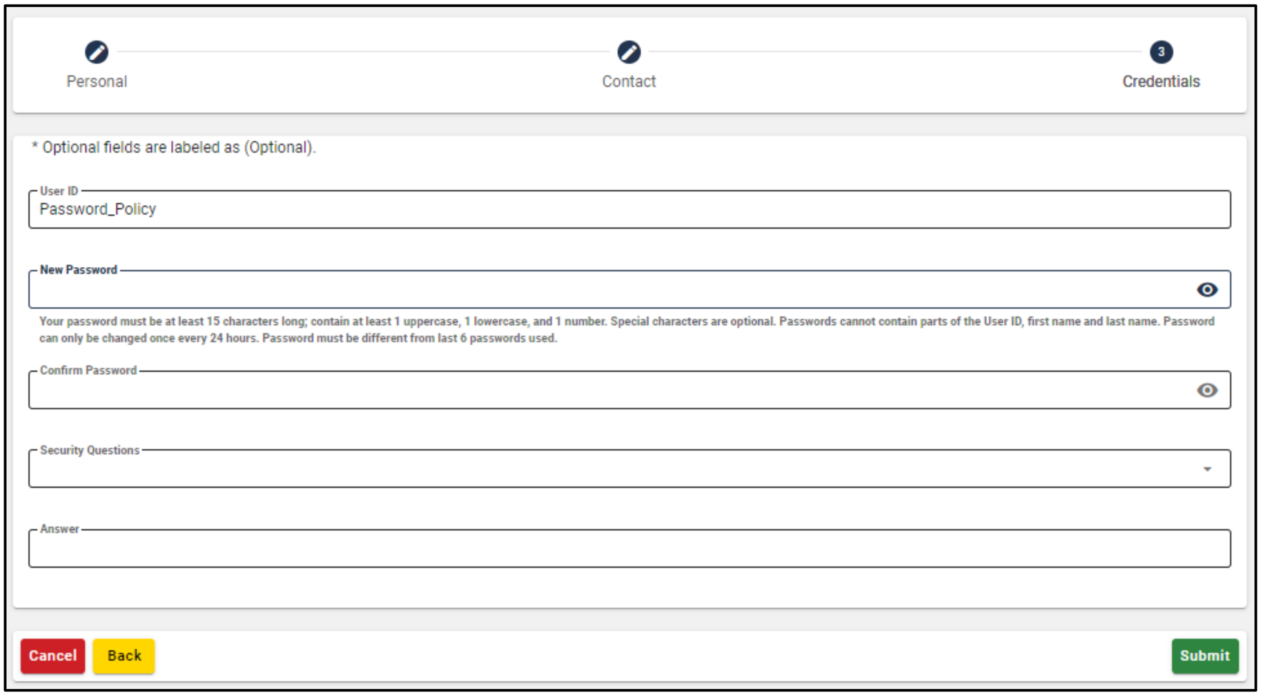
[4] A foreign address is any address that is not located within one of the 50 states or US territories. Users who reside at a foreign address will not be able to use the Remote Identity Proofing (RIDP) process as described in section *13 Remote Identity Proofing*.

[5] The email address that is entered into the Enter Email Address and Confirm E-mail Address fields must be identical or the registration process will not continue.

[6] This email address must be valid and accessible for MFA and other account related notifications.

[7] Users must use the address where they reside as their Home Address. The use of other addresses, such as a business address will cause the RIDP process to fail.

[8] The combination of First Name + Last Name + Email Address must be unique, or the registration process will not continue.



* Optional fields are labeled as (Optional).

User ID: Password_Policy

New Password

Your password must be at least 15 characters long; contain at least 1 uppercase, 1 lowercase, and 1 number. Special characters are optional. Passwords cannot contain parts of the User ID, first name and last name. Password can only be changed once every 24 hours. Password must be different from last 6 passwords used.

Confirm Password

Security Questions

Answer

Figure 3: IDM System User Account Creation Form

7. Enter the desired User ID and Password into the respective fields of the User Account Creation form. [9, 10, 11]
8. Click the Select Challenge Question list box and choose a challenge question from the list that appears.
9. Type the challenge question answer into the Challenge Question Answer field. [12]
10. Click the Submit button to submit the account registration request. The system displays a message that indicates the account was successfully created. [13]

[9] See section *5.1 HDT User ID Policy* for specific User ID requirements for HDT.

[10] The IDM System inspects the User ID to ensure that it is unique. If a user attempts to register with a User ID that is already in use, the system will notify the user that the User ID is already in use.

[11] See section *5.2 HDT Password Policy* for specific password requirements for HDT.

[12] The challenge question answer must be at least four characters long. Additionally, it must not contain parts of the user's first name, last name, password, or challenge question.

[13] Click the Back button to return to the Personal and Contact Information form or click the Cancel link to terminate the new account registration request process.

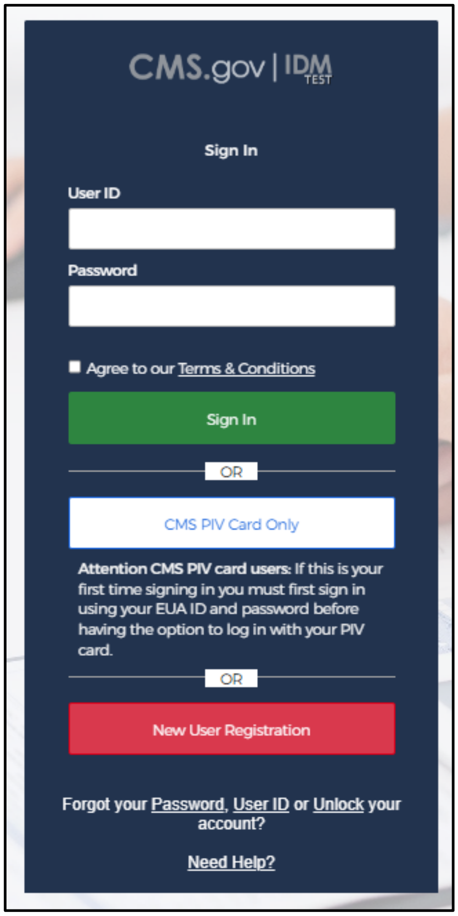
7. How to Sign In to the IDM System

The IDM System authenticates each user and permits them to access the CMS applications to which they have been granted access.

This section provides the steps that users must follow to sign in to the IDM System.

Note: The procedures described in this user guide will use the Email MFA factor when describing login procedures.

1. Navigate to https://home.idm.cms.gov/.



Attention CMS PIV card users: If this is your first time signing in you must first sign in using your EUA ID and password before having the option to log in with your PIV card.

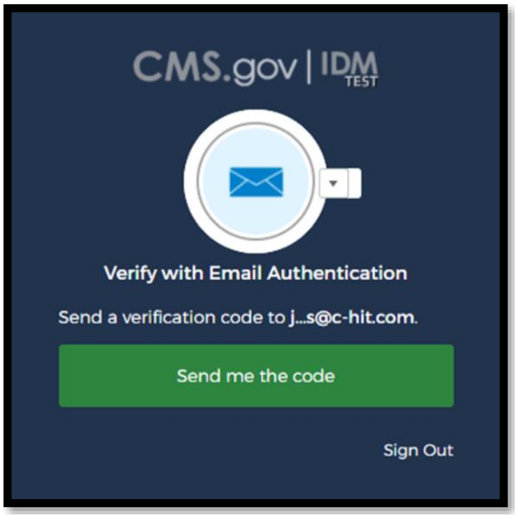
Forgot your Password, User ID or Unlock your account?

Figure 4: IDM System Sign-In UI

2. Enter the Username and Password into the respective fields.
3. Read the Terms & Conditions, click the check box to acknowledge agreement, then click the Sign In button.
4. If prompted, select an MFA factor. [14]

[14] Email is automatically set up as the default MFA factor for all users that are required to log in with MFA.

5. Follow the directions for the chosen MFA factor (MFA device).



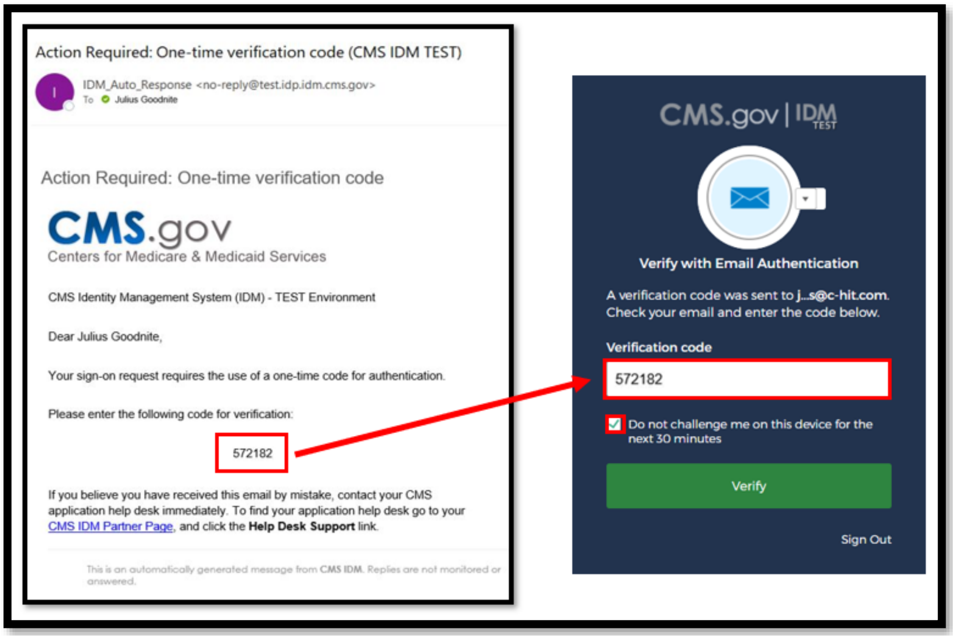
CMS.gov | IDM TEST

Verify with Email Authentication

Send a verification code to j...s@c-hit.com.

Figure 5: Verification Code Request UI

6. When the Verify with Email Authentication UI appears, click the Send me the code button to request a one-time verification code.



Action Required: One-time verification code (CMS IDM TEST)

IDM_Auto_Response <no-reply@test.idp.idm.cms.gov>
To Julius Goodnite

Action Required: One-time verification code

CMS.gov
Centers for Medicare & Medicaid Services

CMS Identity Management System (IDM) - TEST Environment

Dear Julius Goodnite,

Your sign-on request requires the use of a one-time code for authentication.

Please enter the following code for verification:

572182

If you believe you have received this email by mistake, contact your CMS application help desk immediately. To find your application help desk go to your CMS IDM Partner Page, and click the **Help Desk Support** link.

This is an automatically generated message from CMS IDM. Replies are not monitored or answered.

CMS.gov | IDM TEST

Verify with Email Authentication

A verification code was sent to j...s@c-hit.com. Check your email and enter the code below.

Verification code: 572182

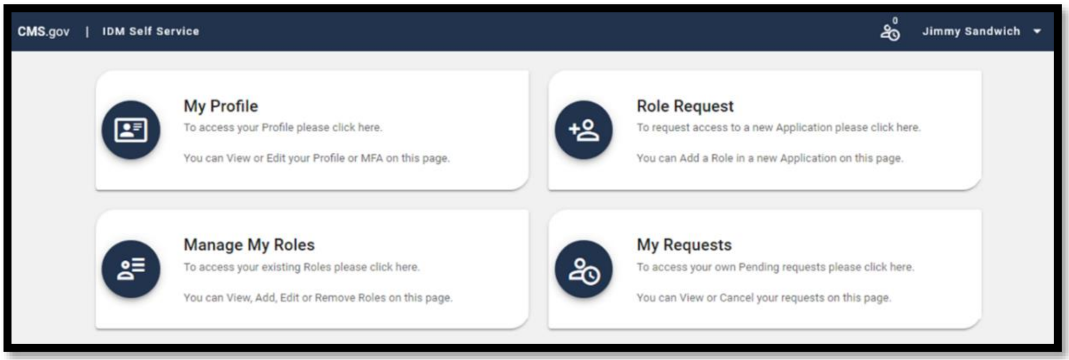
☑ Do not challenge me on this device for the next 30 minutes

Figure 6: One-time Verification Code Email and the Verification Code UI

7. Enter the Verification Code into the Verification Code field. [15]

[15] If the MFA factor uses push notifications, a verification code is not required.

8. (Optional) Click the check box to select the option “Do not challenge me on this device for the next 30 minutes”. [16]
9. Click the Verify button. The user is taken to the IDM Self-Service UI.



My Profile
To access your Profile please click here.
You can View or Edit your Profile or MFA on this page.

Role Request
To request access to a new Application please click here.
You can Add a Role in a new Application on this page.

Manage My Roles
To access your existing Roles please click here.
You can View, Add, Edit or Remove Roles on this page.

My Requests
To access your own Pending requests please click here.
You can View or Cancel your requests on this page.

Figure 7: Dashboard for Users without Approver or Help Desk Capabilities

7.1 How to Overcome Common Sign-In Issues

The IDM System provides self-service features that enable users to address common sign-in issues without requesting assistance from helpdesk personnel. Users may encounter the following issues:

- The user’s password is reset by the MCARE Help Desk.
- The user forgets their password.
- The user’s account is locked.
- The user forgets their User ID.

Note: The procedures described in this user guide will use the Email MFA factor when describing login procedures, self-service password reset procedures, and self-service account unlock procedures.

Users must meet the following conditions to use the self-service procedures to reset their forgotten password or unlock their account as described in this section of the user guide:

- Security Question Answer: The user must remember the security question answer which they established when they created their account.
- Email, IVR, or SMS MFA factor: The user must have an Email, IVR, or SMS MFA factor (MFA device) registered and active in their user profile.

[16] If the checkbox is selected, users will bypass the MFA verification phase of the authentication process if they sign out and sign back into the system again within 30 minutes of completing the initial sign-in procedure.

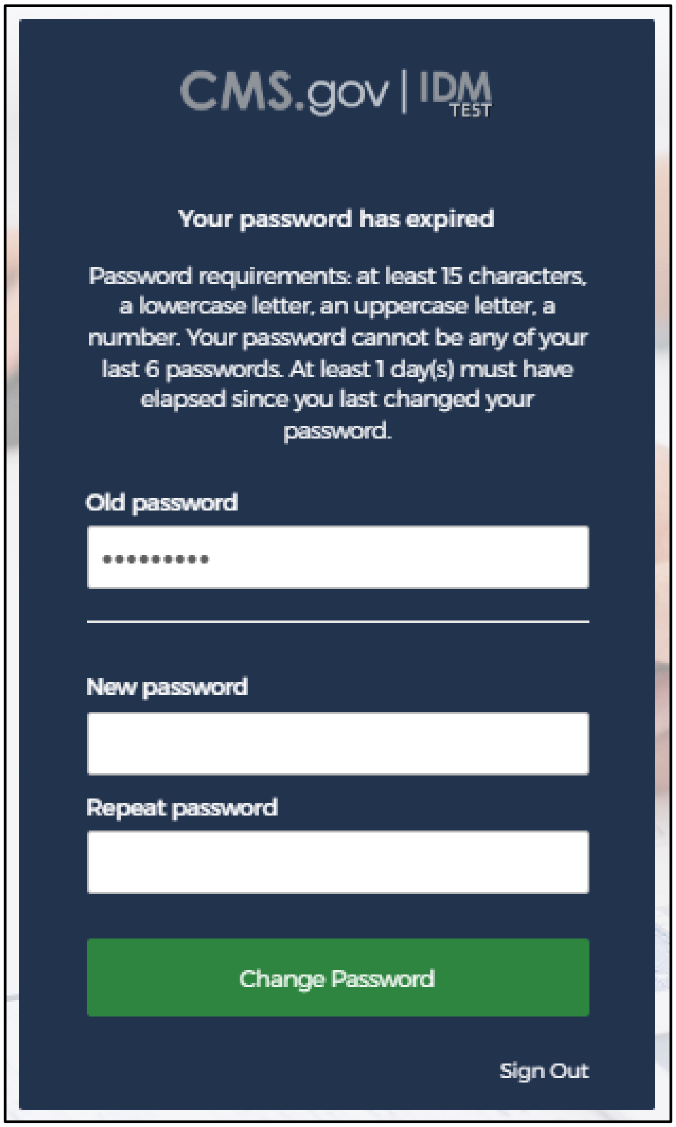
Users who do not meet these conditions will not be able to use these self-service procedures and must contact their respective application helpdesk to obtain assistance. [17]

7.1.1 The User's Password Is Reset

If a user cannot remember their password and/or cannot successfully change the password using self-service options, the Help Desk can force a password reset. This reset then requires the user to change their password at the next login. In this situation, the IDM System Sign-In UI displays a message that informs the user that their password must be changed, as shown in Figure 8. That user is required to create a new password before they can sign in to the IDM System.

This section provides the steps that users must follow to change an expired password.

[17] Users can obtain contact information for their application helpdesk on the CMS Enterprise Portal website's Learn about Your Application Page.



Your password has expired

Password requirements: at least 15 characters, a lowercase letter, an uppercase letter, a number. Your password cannot be any of your last 6 passwords. At least 1 day(s) must have elapsed since you last changed your password.

Old password

••••••••••

New password

Repeat password

Figure 8: IDM Change Password UI

1. Enter the old password into the Old password field.
2. Enter the New password and the Repeat password into the respective fields. [18]
3. Click the Change Password button. [19]

The user can now log in using the new password.

[18] The new password must conform to the guidelines provided in section *5.2 HDT Password Policy*.

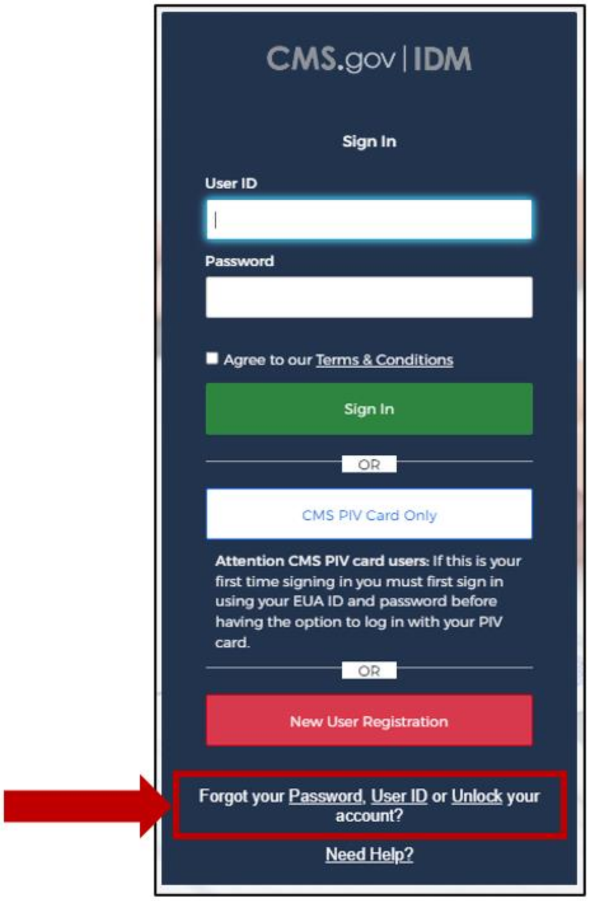
[19] The system sends an email to the user's address on record which indicates that the user's password was changed. It also indicates where the user can obtain assistance if they have questions.

7.1.2 The User Forgets Their Password

The IDM System provides a means for users to reset their own passwords if they are unable to sign in because they forgot their password, provided they meet the conditions outlined in section *7.1 How to Overcome Common Sign-In Issues*.

Users who forget their passwords can reset their own password by using the Forgot your Password link which is located at the bottom of the IDM Sign In UI.

This section provides the steps that users must follow to reset a forgotten password.

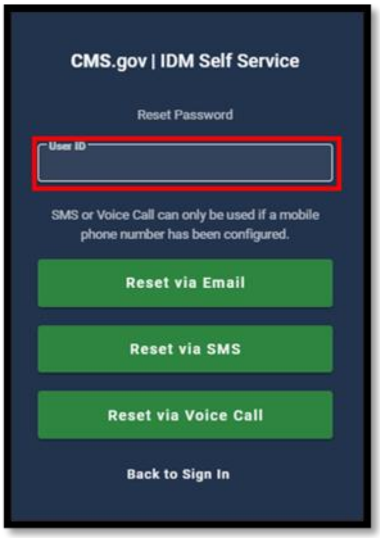


Attention CMS PIV card users: If this is your first time signing in you must first sign in using your EUA ID and password before having the option to log in with your PIV card.

Forgot your Password, User ID or Unlock your account?

Figure 9: IDM System Sign-In UI - Forgotten Password Recovery Link

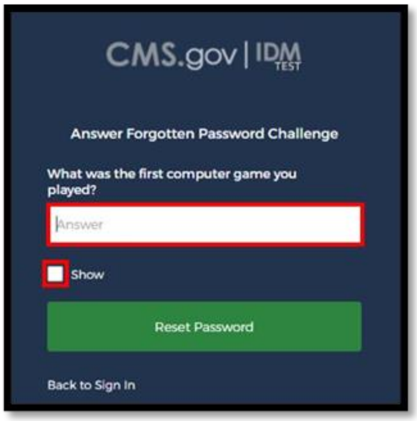
1. Click the Password link located in the lower left corner of the IDM System Sign In UI. The Reset Password UI appears.



SMS or Voice Call can only be used if a mobile phone number has been configured.

Figure 10: IDM System Reset Password UI

2. Enter the User ID in the respective field.
3. Select the button that corresponds to the desired reset method. The reset method will determine how password recovery information is communicated to the user. The Answer Forgotten Password Challenge UI appears. [20, 21, 22]



What was the first computer game you played?

Figure 11: Answer Forgotten Password Challenge UI

4. Enter the security question answer into the field, then click the Reset Password button.[23]
5. The IDM System sends a Forgot Password email to the email address listed in the user’s profile. This email informs the user that a password reset request has been made,

[20] The Reset via Email option is available to all HDT users.

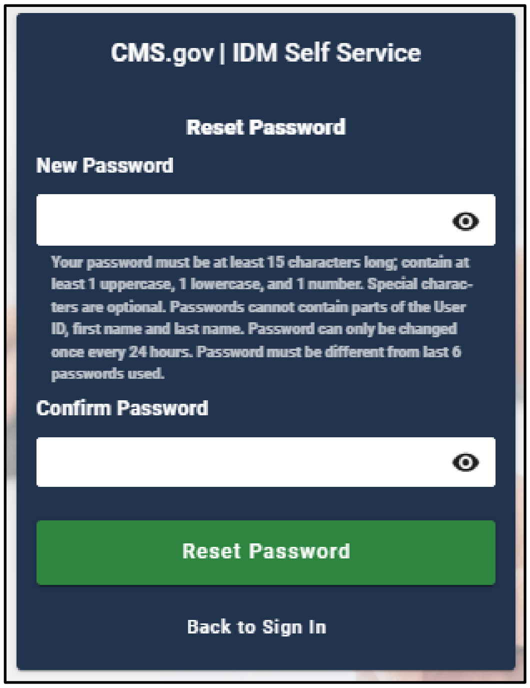
[21] The Reset via SMS option is only available if the user has added a mobile phone number to their user profile and registered that phone number for use with an SMS MFA device.

[22] The Reset via Voice Call option is only available if the user has added a phone number to their user profile and registered that phone number for use with an IVR MFA device.

[23] (Optional) Click the Show check box to view the answer to the security question in clear text.

and it contains a Reset Password hyperlink that the user must use to complete the password reset procedure. [24]

6. Click the Reset Password hyperlink contained within the Forgot Password email. The Reset Your Password UI appears.



CMS.gov | IDM Self Service

Reset Password

New Password

Your password must be at least 15 characters long; contain at least 1 uppercase, 1 lowercase, and 1 number. Special characters are optional. Passwords cannot contain parts of the User ID, first name and last name. Password can only be changed once every 24 hours. Password must be different from last 6 passwords used.

Confirm Password

Figure 12: Reset Your Password UI

7. Enter the New Password and the Repeat Password into the respective fields. [25]
8. Read the Terms & Conditions, then click the check box to acknowledge agreement.
9. Click the Reset Password button. The Verify with Email Authentication UI appears.
10. Click the Send me the code button to request a one-time verification code.
11. The MFA device returns a one-time verification code via email. Enter the one-time verification code into the Verification Code field.
12. (Optional) Click the check box to select the option "Do not challenge me on this device for the next 30 minutes." [26]
13. Click the Verify button. The user is taken to their respective IDM Self-Service UI.

[24] The Reset Password hyperlink expires after four hours have elapsed. The user will be required to repeat this entire procedure if the link expires.

[25] The New Password and Repeat Passwords must match, and both must conform to the guidelines provided in section *5.2 HDT Password Policy*.

[26] If this step is performed, users bypass the MFA verification phase of the authentication process if they sign out and sign back into the system again within 30 minutes of completing this MFA verification event

7.1.3 The User's Account is Locked

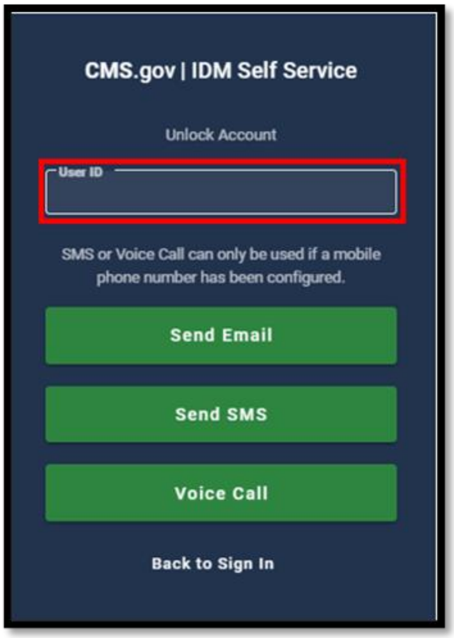
An HDT user's account may be locked for several reasons, some of which require the assistance of MCARE Help Desk personnel to perform a Help Desk-assisted account unlock procedure.

If a user's account gets locked from within the HDT application, then they will receive an on-screen message that includes a specific error code and directions on how to proceed. A complete list of HDT specific account error codes is available in section *18.1 Access and Behavior Error Messages*. Users should follow the on screen recommendations. When directed to do so, users should take note of the error message they received and then contact the MCARE Help Desk for assistance. Refer to section *17.3 Support Information* for MCARE Help Desk contact information.

If a user's account gets locked when the user exceeds the maximum number of failed sign-in attempts, that is an IDM System account lock and the user may use the self-service procedure described in this section, provided they meet the conditions outlined in section *7.1 How to Overcome Common Sign-In Issues*.

Such users can use the Unlock your account link which is located at the bottom of the IDM Sign-In UI.

This section provides the steps that users must follow if they exceed the maximum number of failed IDM sign-in attempts and thus lock their IDM account.



CMS.gov | IDM Self Service

Unlock Account

User ID

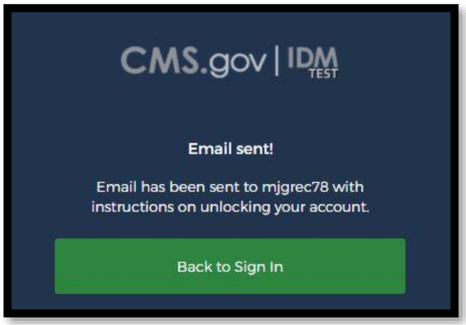
SMS or Voice Call can only be used if a mobile phone number has been configured.

Figure 13: IDM System Unlock Account UI

1. The Unlock Account UI appears whenever a user enters their credentials and tries to sign in after the account is locked for excessive failed sign-in attempts. The IDM System

also sends an Account Locked email that explains why the account was locked and steps the user should take to unlock the account. [27]

2. Enter the User ID in the User ID field.
3. Select the button on the Unlock Account UI that corresponds to the desired unlock method. The Unlock Account UI is illustrated in Figure 13: IDM System Unlock Account UI. The unlock method will determine how password recovery information is communicated to the user. [28, 29, 30]



CMS.gov | IDM TEST

Email sent!

Email has been sent to mjgrec78 with instructions on unlocking your account.

Figure 14: Unlock Request Sent UI

4. When the Unlock Request Sent UI appears, click the Back to Sign In button.
5. The IDM System sends an Account Unlock Request email to the email address listed in the user's profile. This email informs the user that an account unlock request has been made, and it contains an Unlock Account hyperlink that the user must use to complete the Unlock Account procedure. [31]
6. Click the Unlock Account hyperlink contained within the Account Unlock email. The Answer Unlock Account Challenge UI appears.

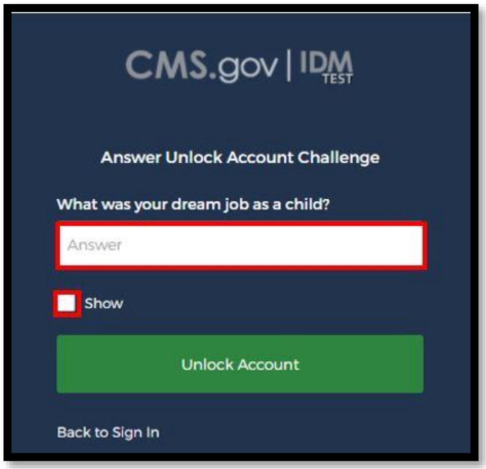
[27] The user can also click the Unlock your account link that is located on the bottom of the IDM System Sign In window as shown in Figure 4: IDM System Sign-In UI.

[28] The Unlock via Email option is available to all HDT users.

[29] The Unlock via SMS option is only available if the user has added a mobile phone number to their user profile and registered that phone number for use with an SMS MFA device.

[30] The Unlock via Voice Call option is only available if the user has added a phone number to their user profile and registered that phone number for use with an IVR MFA device.

[31] The Unlock Account hyperlink expires after four hours have elapsed. The user will be required to repeat this entire procedure if the link expires.



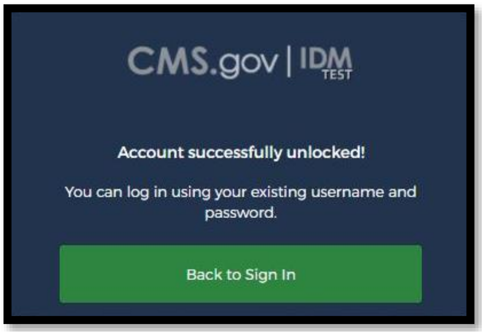
CMS.gov | IDM TEST

Answer Unlock Account Challenge

What was your dream job as a child?

Figure 15: Answer Unlock Account Challenge Question UI

7. Type the answer to the challenge question into the field, then click the Unlock Account button. If the user answers the question correctly, the Account Successfully Unlocked UI appears. [32]



CMS.gov | IDM TEST

Account successfully unlocked!

You can log in using your existing username and password.

Figure 16: Account Successfully Unlocked UI

8. Click the Back to Sign In button. The IDM System Sign-In UI appears, and the user's account is now unlocked. [33]

[32] (Optional) Click the Show check box to view the answer to the security question in clear text.

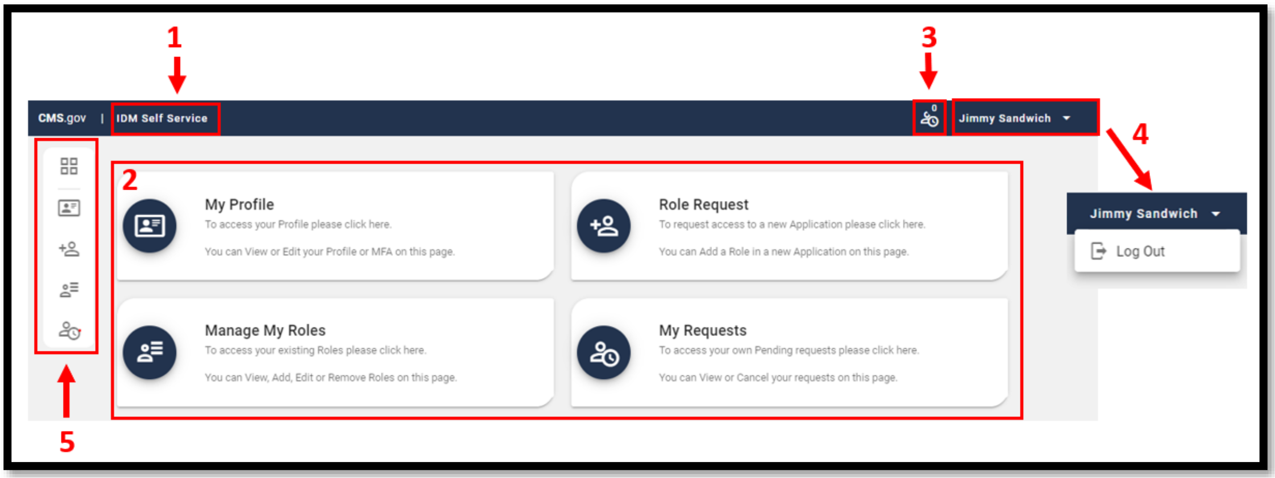
[33] The user can attempt to sign in with their existing password if they remember it using the procedure described in section *7 How to Sign In to the IDM System*, or they can use the self-service password reset procedure described in section *7.1.2 The User Forgets Their Password*.

8. The IDM Self-Service UI

8.1 Overview of the IDM Self-Service UI

The IDM Self-Service UI provides access to self-service functions that allow users to manage their user profile, request new applications, and manage roles for applications to which they have been granted access. Table 3: Summary of Common Self-Service UI Controls and Features provides a summary of the features and controls that are available on the Self-Service UI for HDT users. [34]

Figure 17: IDM Self-Service UI for Users without Approver or Help Desk Capabilities illustrates the IDM Self-Service Dashboard. The functions shown represent the minimum number of functions that are available to all users.



To access your Profile please click here.

You can View or Edit your Profile or MFA on this page.

To request access to a new Application please click here.

You can Add a Role in a new Application on this page.

To access your existing Roles please click here.

You can View, Add, Edit or Remove Roles on this page.

To access your own Pending requests please click here.

You can View or Cancel your requests on this page.

Figure 17: IDM Self-Service UI for Users without Approver or Help Desk Capabilities

Table 3: Summary of Common Self-Service UI Controls and Features

Reference	Control Name	Description
1	IDM Self-Service Button	This control returns the user to the IDM Self-Service UI.
2	IDM Self-Service Function Buttons	These controls launch the various functions that can be accessed through the IDM Self-Service UI. • All users have access to these buttons.
3	My Requests Counter	This indicator displays the number of pending requests that have been submitted by the currently logged in user and provides 1-click access to a summary of those requests.
4	Dropdown Menu	This control displays the currently logged in user and provides access to the Log Out function when clicked.

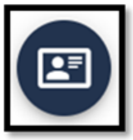
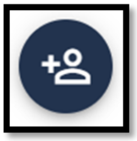
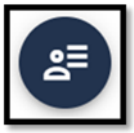
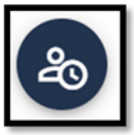
[34] Users that possess additional capabilities have access to additional Self-Service UI functions whose controls are only displayed to those individuals.

Reference	Control Name	Description
5	Self Service Taskbar	This is a dynamic control which appears whenever a user accesses one of the Self-Service functions. This control enables the user to move between the various Self-Service functions which can be accessed through the Self-Service UI.

8.2 Description of Functions Common to all Users

Table 4: IDM System Self-Service Functions Common to all Users contains a description of the Self-Service functions that are available to all users of the IDM System.

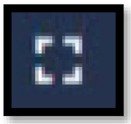
Table 4: IDM System Self-Service Functions Common to all Users

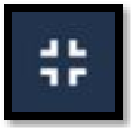
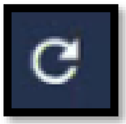
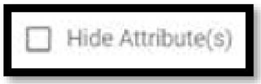
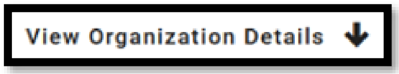
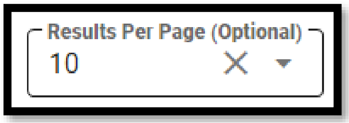
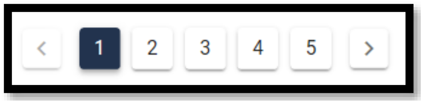
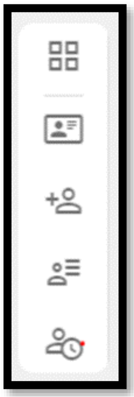
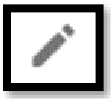
Function Name	Icon	Function Description
My Profile		This function enables the currently logged in user to view and edit their profile. • Profile information can also be accessed using the **My Profile** taskbar option.
Role Request		This function enables the currently logged in user to request access to a new application. • Requests for access to new or existing applications can also be submitted using the **Role Request** taskbar option.
Manage My Roles		This function enables the currently logged in user to manage existing roles. • User can view, add, edit, or remove roles. • Roles can also be managed using the **Manage My Roles** taskbar option.
My Requests		This function enables the currently logged in user to access their own pending requests. • Users can view or cancel requests. • Pending request information can also be accessed using the **My Requests** taskbar option.

8.3 Description of the Self-Service UI Common Controls

Table 5: Self-Service UI Common Controls contains a description of the common controls that are used by all functions that can be accessed from the Self-Service UI.

Table 5: Self-Service UI Common Controls

Control Name	Icon	Function
Full-screen View		This control places the UI in full-screen view.

Control Name	Icon	Function
Normal View		This control exits full-screen view and places the UI in normal view.
Refresh		This control refreshes the list of records displayed on the screen.
Hide Attribute(s)		This control provides the option to hide the Attribute and Additional Details columns.
View Details		This control displays additional detail information about the request. These details are displayed within the results page. • This is a dynamic control which displays a label and details that change according to role attribute information. • This control will not appear for applications that do not have role attributes.
Pagination		This control enables the user to select the number of records (results) that are displayed as a "page" on the screen.
Page Selector		This control permits the user to select a specific page of results to view. • The user can change the page size using the Pagination control.
Self Service Taskbar		This control provides users with 1-click access to each Self-Service function that the currently logged in user has access to. • The taskbar dynamically appears in the upper left corner of the Self-Service UI when one of the Self-Service functions is being used.
Edit		The control allows the user to edit various information that is stored in the user's profile.

9. How to Use the IDM My Profile Function

Users can view and edit their user profile information using the My Profile button located on the Self-Service UI or the My Profile taskbar option.

9.1 Description of the IDM My Profile Function

The My Profile function enables users to view and/or modify various attributes of their user profile. Users may perform the following profile management tasks:

- View a summary of their user profile
- Modify their Personal Contact Information
- Modify their Business Contact Information
- Change their password
- Change their security question
- Manage their MFA devices

Table 6: User Profile Information Categories contains a list of the categories of information that comprise the user profile, their respective data elements (when available), and user actions that may be performed on those categories of information.

Table 6: User Profile Information Categories

Category	Data Elements	Action
My Information	User ID Title First Name Middle Name Last Name Suffix Date of Birth Last 4 of SSN	View only
Personal Contact Information	E-Mail Address Address Line 1 & Line 2 City State Zip Code & Zip Code Extension Phone Number	View and modify
Business Contact Information	Professional Credentials Company Name Company Address Line 1 & Line 2 City State Zip Code & Zip Code Extension Company Phone & Company Phone Extension Office Phone & Office Phone Extension	View and modify

Category	Data Elements	Action
Change Password	Current Password New Password Confirm Password	Change user password
Change Security Question	Security Questions Answer Current Password	Change security question and answer
Manage MFA Devices	MFA Device Properties: • Type • Value • Status	Add/Remove/Modify MFA device attributes

9.2 How to Launch and Close the IDM My Profile Function

Launch the My Profile Function:

1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option.

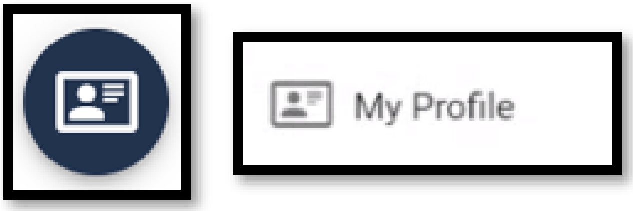


Figure 18: My Profile Button and My Profile Taskbar Option

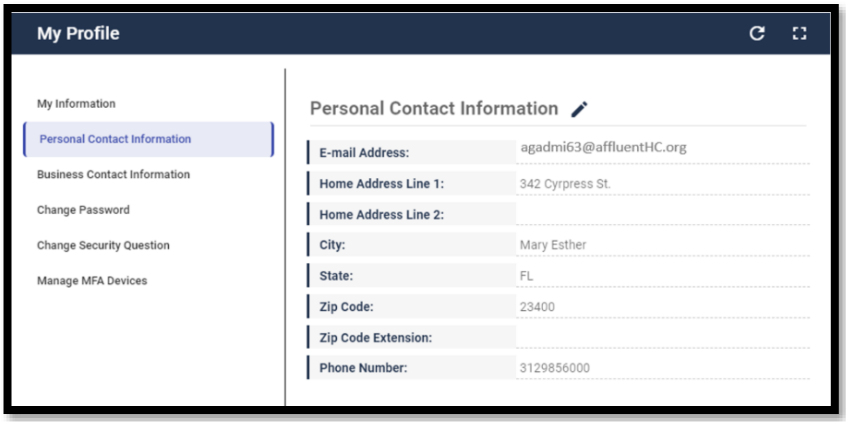
Close the My Profile Function:

1. Choose one of the following actions to close the My Profile function:
   - Click the IDM Self-Service button located at the top left of the Self-Service UI.
   - Select another function from the Self-Service taskbar.
   - Select the Log Out option from the dropdown menu and log out of the system.

9.3 How to View IDM User Profile Information

The My Information UI displays a read-only summary of the currently signed in user’s profile information.

The My Information UI displays as soon as the user launches the My Profile function using the procedure described in section *9.2 How to Launch and Close the IDM My Profile Function*.



Personal Contact Information

E-mail Address:	agadmi63@affluentHC.org
Home Address Line 1:	342 Cyrpress St.
Home Address Line 2:	
City:	Mary Esther
State:	FL
Zip Code:	23400
Zip Code Extension:	
Phone Number:	3129856000

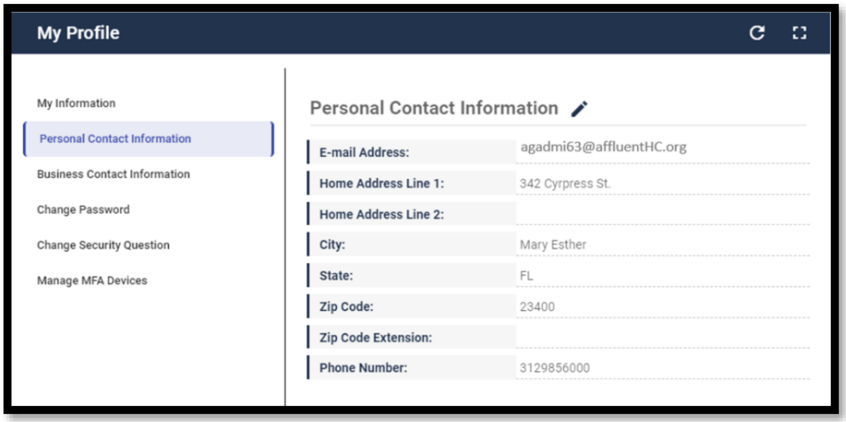
Figure 19: My Profile - My Information

9.4 How to View and Edit IDM User Personal Contact Information

This section provides the steps that users must follow to view and edit the personal contact information of the user that is currently logged in.

View Personal Contact Information

1. Click the My Profile button located on the Self-Service UI or Click the My Profile taskbar option. These controls are shown in Figure 20: My Profile - Personal Contact Information.



Personal Contact Information

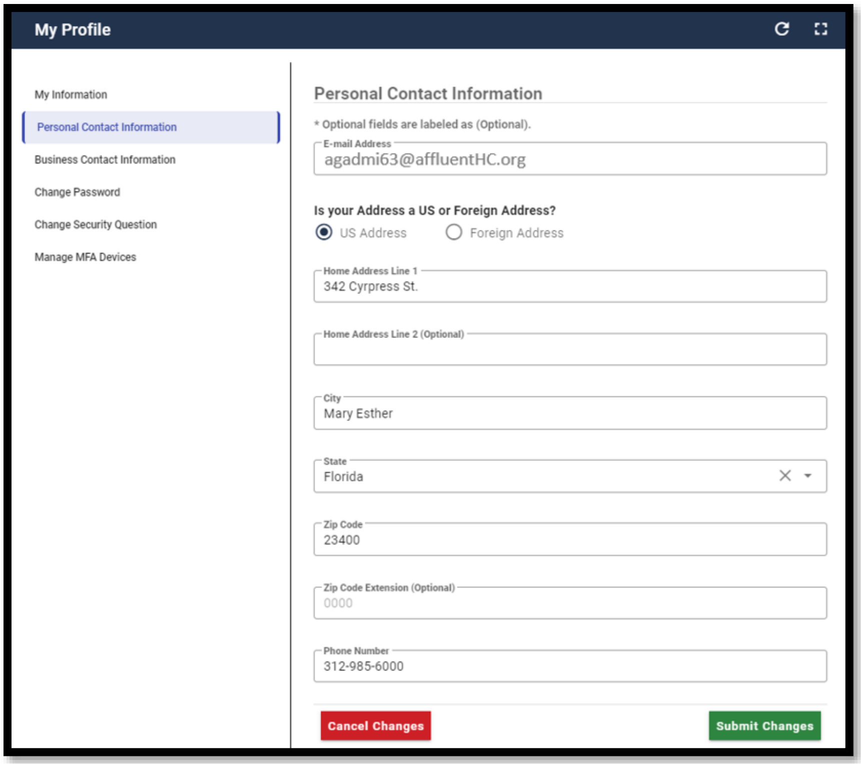
E-mail Address:	agadmi63@affluentHC.org
Home Address Line 1:	342 Cyrpress St.
Home Address Line 2:	
City:	Mary Esther
State:	FL
Zip Code:	23400
Zip Code Extension:	
Phone Number:	3129856000

Figure 20: My Profile - Personal Contact Information

2. Click the Personal Contact Information link to open the Personal Contact Information UI and view the currently logged in user's personal contact information.

Edit Personal Contact Information

1. With the Personal Contact Information UI open, click the Personal Contact Information edit control. ✎ The Personal Contact Information form will open.



Personal Contact Information

* Optional fields are labeled as (Optional).

E-mail Address: agadmi63@affluentHC.org

Is your Address a US or Foreign Address?
● US Address ○ Foreign Address

Home Address Line 1: 342 Cyrpress St.

Home Address Line 2 (Optional):

City: Mary Esther

State: Florida

Zip Code: 23400

Zip Code Extension (Optional): 0000

Phone Number: 312-985-6000

Figure 21: My Profile - Edit Personal Contact Information Form

2. Make the desired changes, then click the Submit Changes button. The Personal Contact Information UI appears and displays the recent changes. [35, 36, 37]

9.5 How to View and Edit IDM User Business Contact Information

This section provides the steps that users must follow to view and edit the business contact information of the user that is currently logged in.

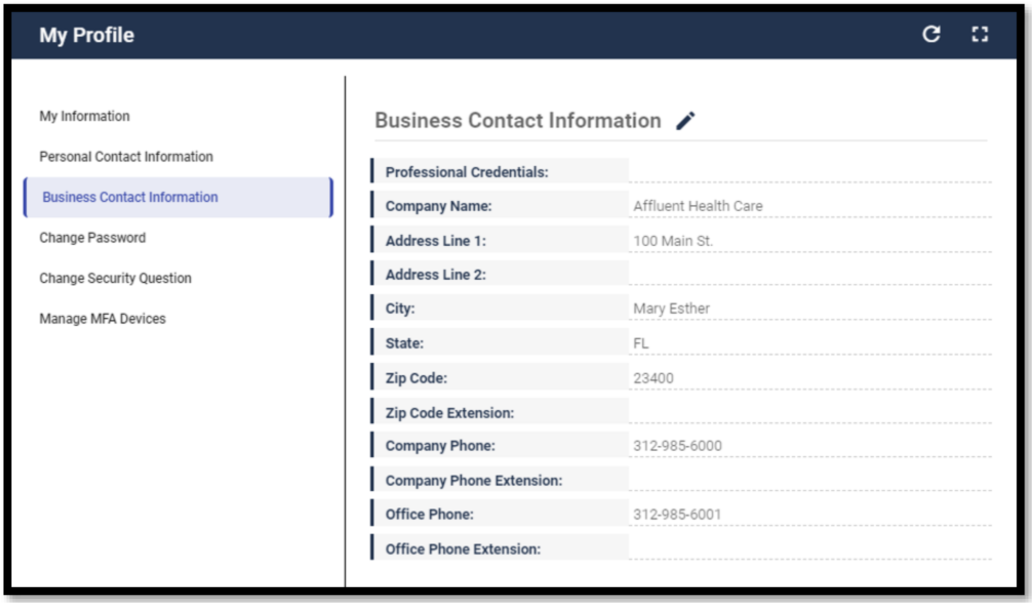
[35] A user account is considered duplicate when the combination of First Name + Last Name + Email Address as changed already exists in the system.

[36] An email is sent to the user’s email address of record which indicates a change to their information has occurred. If the user changed their email address, the email will be sent to both the old and new email addresses.

[37] Click the Cancel Changes button to discard changes to the personal contact information.

View Business Contact Information

1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.



My Profile

Business Contact Information ✎

Professional Credentials:

Company Name: Affluent Health Care

Address Line 1: 100 Main St.

Address Line 2:

City: Mary Esther

State: FL

Zip Code: 23400

Zip Code Extension:

Company Phone: 312-985-6000

Company Phone Extension:

Office Phone: 312-985-6001

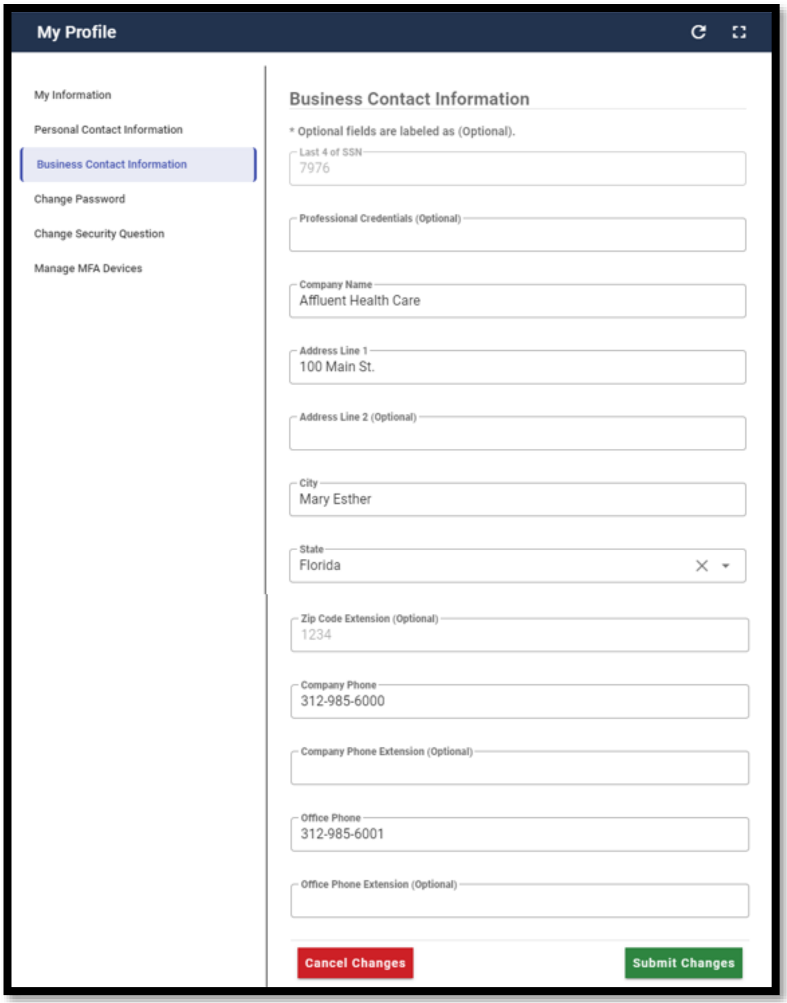
Office Phone Extension:

Figure 22: My Profile - Business Contact Information

2. Click the Business Contact Information link to open the Business Contact Information UI and view the currently logged in user's business contact information.

Edit the User's Business Contact Information

1. With the Business Contact Information UI open, click the Business Contact Information edit control. ✎ The Business Contact Information form will open.



Business Contact Information

* Optional fields are labeled as (Optional).

Last 4 of SSN: 7976

Professional Credentials (Optional):

Company Name: Affluent Health Care

Address Line 1: 100 Main St.

Address Line 2 (Optional):

City: Mary Esther

State: Florida

Zip Code Extension (Optional): 1234

Company Phone: 312-985-6000

Company Phone Extension (Optional):

Office Phone: 312-985-6001

Office Phone Extension (Optional):

Figure 23: My Profile - Edit Business Contact Information Form

2. Make the desired changes, then click the Submit Changes button. The Personal Contact Information UI appears and displays the recent changes. [38, 39]

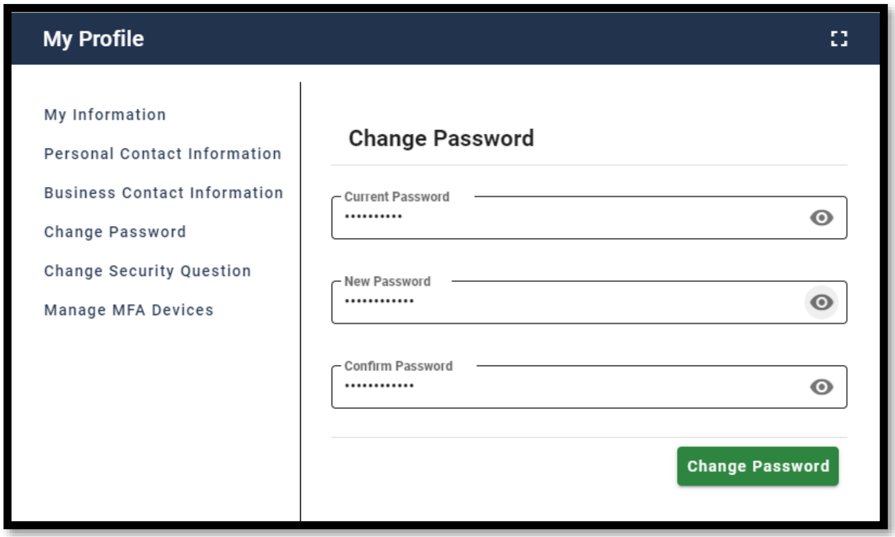
9.6 How to Change the IDM User Account Password

The Change Password form enables the currently logged in user to change their password. This section provides the steps that the user must follow to change their password.

1. Click the My Profile button located on the Self-Service UI or Click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Change Password link. The Change Password form opens.

[38] An email is sent to the user's email address of record which indicates that a change to their information has occurred.

[39] Click the Cancel Changes button to discard changes to the personal contact information.



Current Password ••••••••••

New Password ••••••••••••

Confirm Password ••••••••••••

Figure 24: My Profile - Change Password Form

3. Type the current password into the Current Password field.
4. Type the New Password and the Confirm Password into the respective fields. [40]
5. Click the Change Password button. [41]

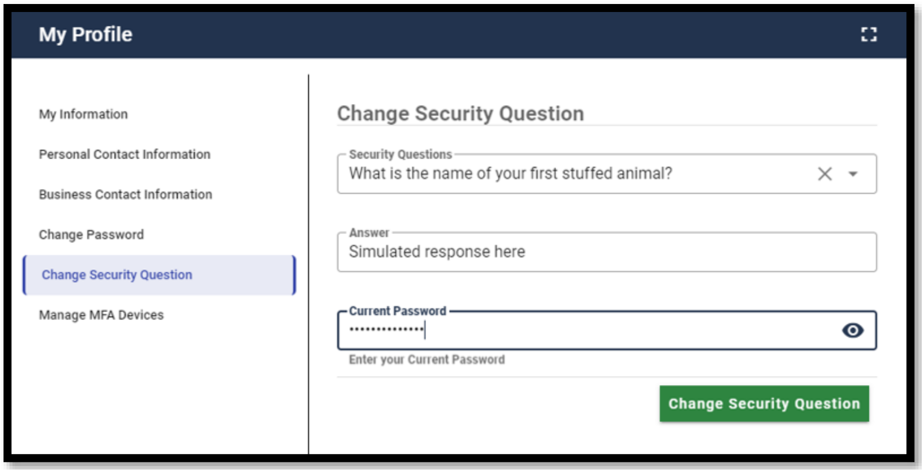
9.7 How to Change the IDM User Security Question

The Change Security Question form enables the currently logged in user to change their password. This section provides the steps that the user must follow to change their security question.

1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Change Security Question link. The Change Security Question form opens.

[40] The new password must conform to the guidelines provided in section *5.2 HDT Password Policy*.

[41] An email is sent to the user's email address of record which indicates that the password change was successful.



Security Questions: What is the name of your first stuffed animal?

Answer: Simulated response here

Current Password: ••••••••••••••

Enter your Current Password

Figure 25: My Profile - Change Security Question Form

3. Click the Security Questions drop down menu and select a security question.
4. Type the security question answer into the Answer field. [42]
5. Type the current password into the Current Password field.
6. Click the Change Security Question button. [43]

9.8 How to Manage IDM MFA Devices

The Manage MFA Devices function provides users with the ability to manage their MFA devices. The following device management tasks can be performed:

- Display active MFA devices.
- Add a new MFA device.
- Edit MFA device settings. [44]
- Remove an MFA device.

Table 7: Manage MFA Devices Function Controls describes the controls that are used by the Manage MFA Devices Function. These controls are used in addition to the common controls listed in Table 5: Self-Service UI Common Controls.

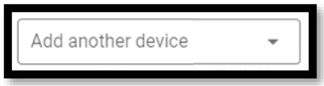
Table 7: Manage MFA Devices Function Controls

Control Name	Icon	Function
Edit Information	✎	This control is used to edit specific information fields in the user's profile that control MFA device settings.

[42] The security question answer must be at least four characters long. Additionally, it must not contain parts of the user's first name, last name, password, or security question.

[43] The IDM System sends a security question change email notification to the email address listed in the user's profile to indicate that the security question change was successful.

[44] Only Email MFA device settings can be edited. Other MFA devices must be removed and then added again using the new settings.

Control Name	Icon	Function
Edit Factor	👤✎	This control opens a UI that enables a user to modify the information that the MFA device uses to communicate with the user.
Activate Factor	👤✎	This control opens a UI that enables a user to request a code that is used to activate an MFA device that is currently in a Pending state.
Remove Factor	×👤	This control removes the MFA device from the user's profile. The email MFA device cannot be removed.
Add Another Device	 Add another device ▾	This control provides a dropdown list that enables the user to select a new MFA device type to add to their account.

9.8.1 How to View Active MFA Devices

A user may have multiple active MFA devices attached to their account if they desire. Active MFA devices can be viewed in two places:

- **The Authentication Factor selection drop-down list**: This list appears during the IDM System sign in process. [45, 46]
- **The Manage MFA Devices UI**: This UI is accessed through the Self-Service UI using the My Profile function. It displays device information that is stored in the user's profile.

When a user has multiple active MFA factors attached to their account, they have the option to choose which one they wish to use when they sign in to the IDM System.

[45] Email is automatically set up as the default MFA factor for all HDT users. No further action is necessary by users to set up email as their MFA factor.

[46] The dropdown control and dropdown list are only visible if the user has two or more active MFA factors registered to their profile.

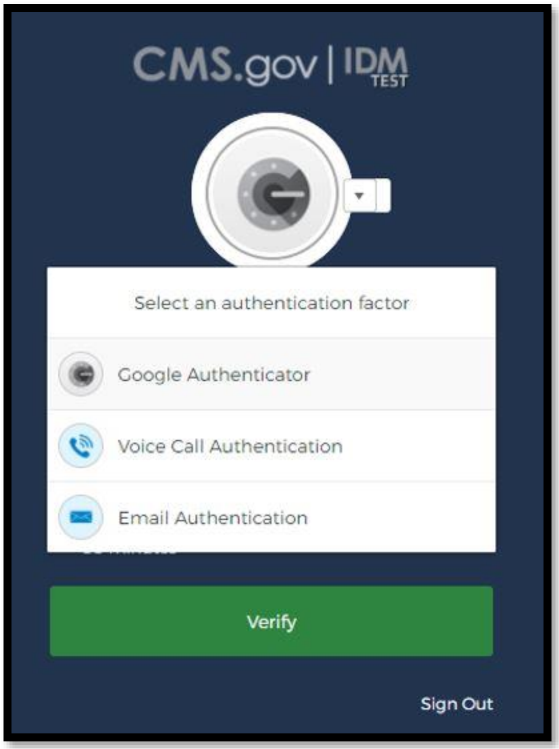


Figure 26: Active MFA Factor (Authentication Factor) Selection List

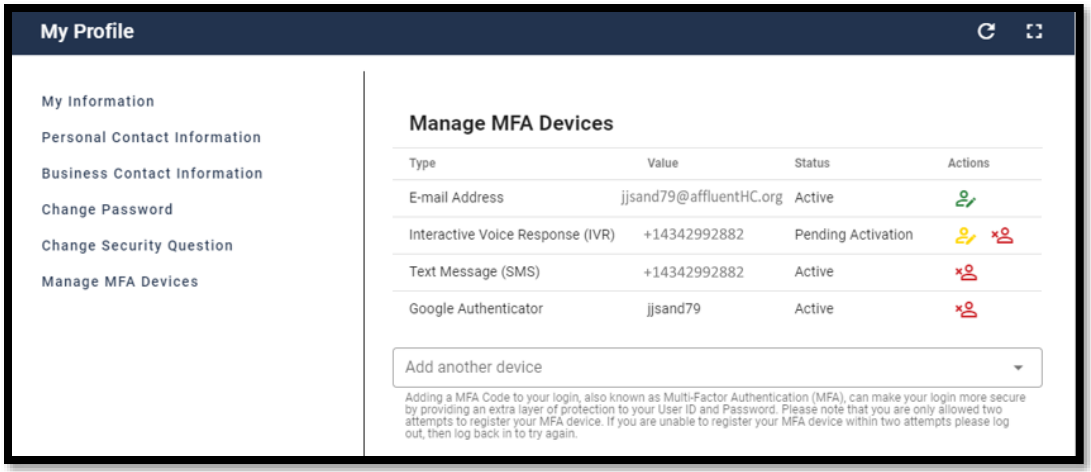
The procedure below enables users to view active MFA factors that are registered to their profiles using the My Profile function.

1. Click the My Profile button located on the Self-Service UI or Click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Manage MFA Devices link. The Manage MFA Devices function opens and displays a summary of all active MFA devices that are registered to the user's profile. [47, 48, 49]

[47] The type represents the MFA device type. IDM currently supports Email, Interactive Voice Response (IVR), Google Authenticator, Okta Verify, and Short Message Service (SMS) Text Message MFA device types.

[48] The value represents the personal contact identifier that the MFA device uses to communicate authentication information.

[49] Migrated HDT users will automatically have an Email MFA device assigned to their user account.



Manage MFA Devices

Type	Value	Status	Actions
E-mail Address	jjsand79@affluentHC.org	Active	
Interactive Voice Response (IVR)	+14342992882	Pending Activation	
Text Message (SMS)	+14342992882	Active	
Google Authenticator	jjsand79	Active	

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 27: Manage MFA Devices Function

Table 8: Summary of MFA Device Management Actions provides a summary of the management actions that a user can perform on each MFA device type.

Table 8: Summary of MFA Device Management Actions

MFA Device	Actions	Modifiable Setting	Notes
Email	Edit	Email Address	Redirects to Change Profile.
Text Message (SMS)	Add/Activate, or Remove	Mobile Phone Number	Activate resolves a pending state.
Interactive Voice Response (IVR)	Add/Activate, or Remove	Phone Number	Activate resolves a pending state.
Google Authenticator	Add or Remove	N/A	Edit is not applicable.
Okta Verify	Add or Remove	N/A	Edit is not applicable.

9.8.2 How to Add an IVR or a SMS MFA Device

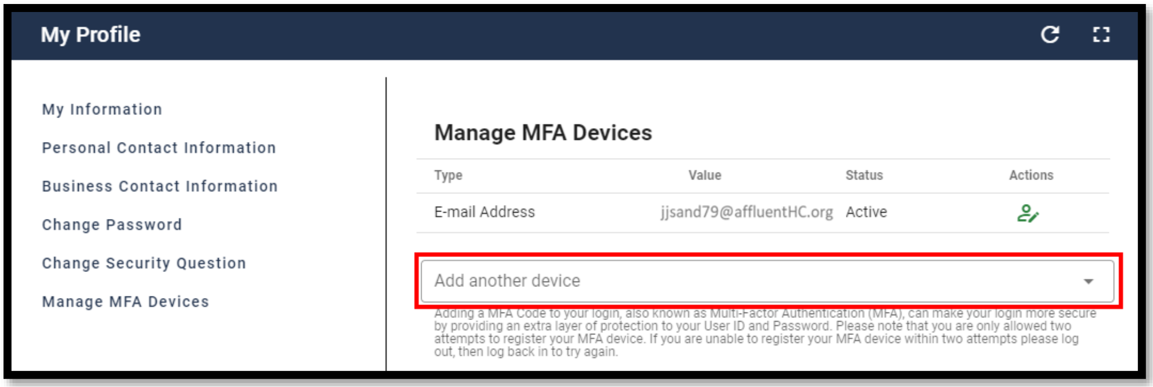
An IVR MFA device delivers a one-time verification code using an automated voice message that is sent directly to the phone number the user provides when the device is added to the user account.

An SMS MFA device delivers a one-time verification code using a text message that is sent directly to the phone number the user provides when the device is added to the user account.

This section provides the steps that users must follow to add an IVR MFA or a SMS MFA device to the user's account. [50]

1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Manage MFA Devices link. The Manage MFA Devices function opens.

[50] The user may add both an IVR MFA device and a SMS MFA device to their account if they desire.



Manage MFA Devices

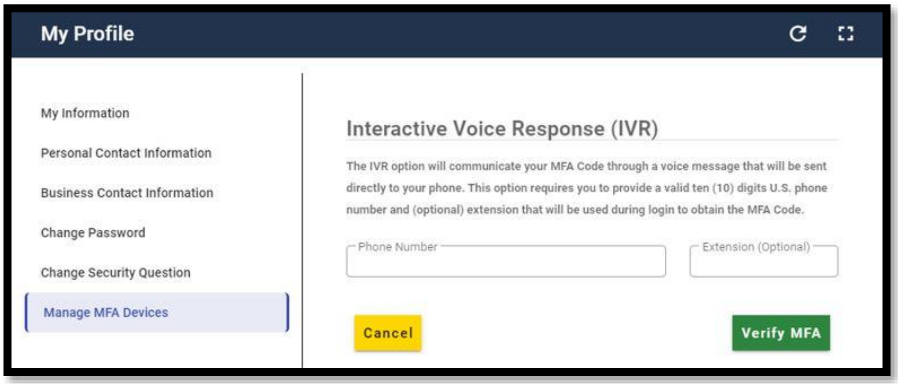
Type	Value	Status	Actions
E-mail Address	jjsand79@affluentHC.org	Active	

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 28: Manage MFA Devices - Option to Add Another Device

3. Click the Add another device drop-down menu and select the Interactive Voice Response (IVR) option or Text Message (SMS) option. The IVR MFA device configuration form or the SMS MFA device configuration form will open.



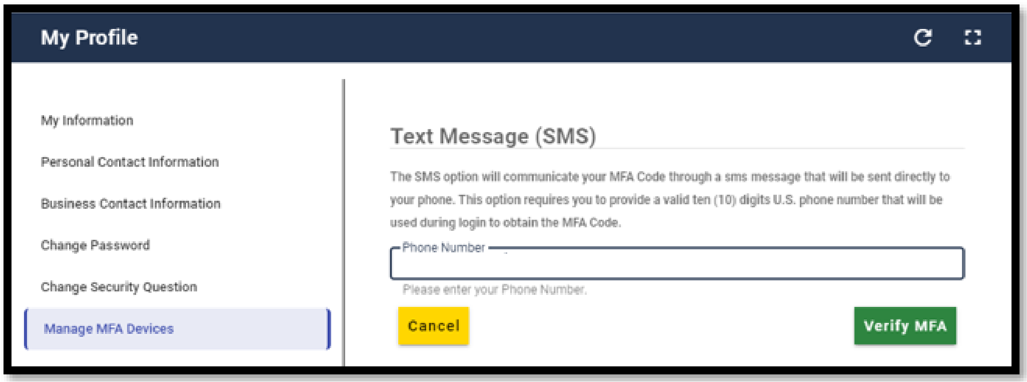
Interactive Voice Response (IVR)

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.

Phone Number

Extension (Optional)

Figure 29: IVR MFA Device Configuration Form



Text Message (SMS)

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.

Phone Number

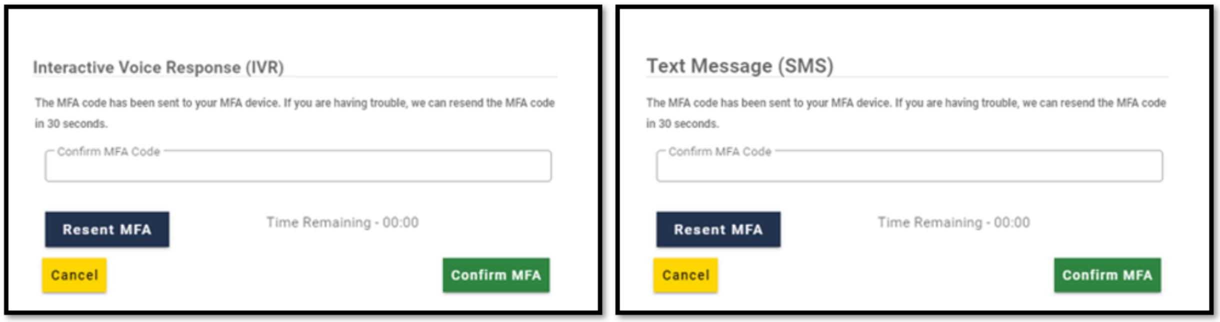
Please enter your Phone Number.

Figure 30: Text Message (SMS) MFA Device Configuration Form

4. Type the Phone Number into the Phone Number field. [51]

[51] For IVR MFA devices, type the Extension (if required) into the Extension field.

5. Click the Verify MFA button. The IVR MFA confirmation UI or the SMS MFA confirmation UI appears.



Interactive Voice Response (IVR)

The MFA code has been sent to your MFA device. If you are having trouble, we can resend the MFA code in 30 seconds.

Confirm MFA Code

Time Remaining - 00:00

Text Message (SMS)

The MFA code has been sent to your MFA device. If you are having trouble, we can resend the MFA code in 30 seconds.

Confirm MFA Code

Time Remaining - 00:00

Figure 31: IVR and SMS MFA Confirmation UIs

The IDM System places an automated voice call or sends a text message to the phone number that was provided in the configuration form. The automated voice call or text message communicates a one-time verification code to the user. [52]

6. Type the one-time verification code into the Confirm MFA Code field and click the Confirm MFA button. [53, 54]
7. Click the OK button. [55]

9.8.3 How to Activate an IVR or a SMS MFA Device

This section provides the steps that users must follow to activate an IVR MFA device that is in a pending state.

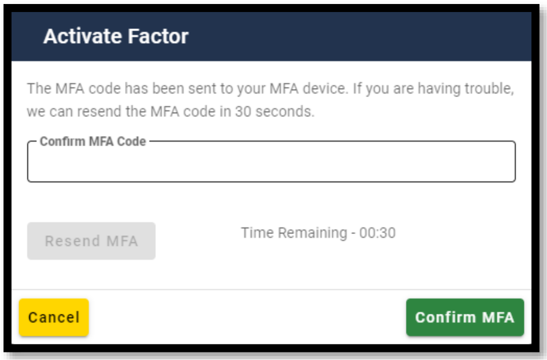
1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Manage MFA Devices link. The Manage MFA Devices function opens.
3. Click the Activate Factor control for the MFA device that requires activation. The Activate Factor UI opens.

[52] (Optional) Click the Resend MFA button if a voice call or text message is not received after 30 seconds has elapsed.

[53] A message is displayed which indicates the MFA device was correctly added.

[54] If the user clicks the Cancel button instead of entering the one-time verification code, the respective device will be placed in a Pending state and its status will reflect Pending in the Manage MFA Devices window. The device will need to be activated using the procedure in section *9.8.3 How to Activate an IVR or a SMS MFA Device*.

[55] An email is sent to the user's email address of record which indicates that an MFA device has been added to the account and the new MFA device appears as an optional authentication factor the next time the user signs in.



Activate Factor

The MFA code has been sent to your MFA device. If you are having trouble, we can resend the MFA code in 30 seconds.

Confirm MFA Code

Time Remaining - 00:30

Figure 32: Activate Factor UI

4. The IDM System places an automated voice call or sends a text message to the phone number that was provided in the configuration form. The automated voice call or text message communicates a one-time verification code to the user. [56]
5. Type the one-time verification code into the Confirm MFA Code field and click the Confirm MFA button. [57, 58]
6. Click the OK button. [59]

9.8.4 How to Add a Google Authenticator Browser Plugin MFA Device

The Google Authenticator MFA device uses the Google Authenticator Chrome browser plugin to deliver a one-time verification code to the user's desktop or laptop computing device.

This section provides the steps that users must follow to add a Google Authenticator Chrome browser plugin MFA device to the user's account.

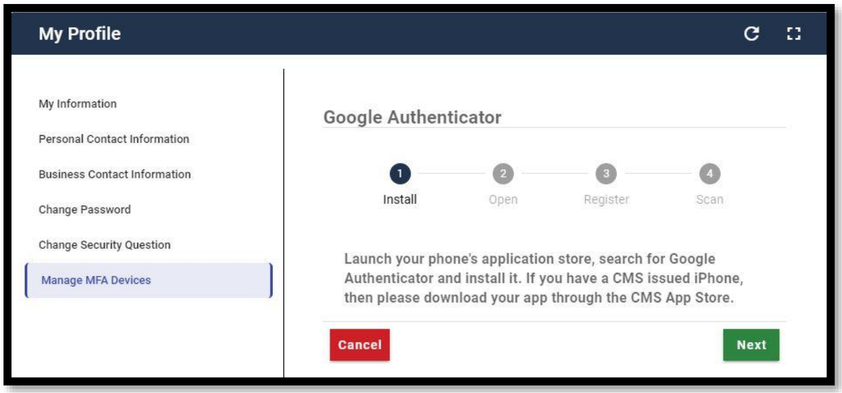
1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Manage MFA Devices link. The Manage MFA Devices function opens.
3. Click the Add another device drop-down control and select the Google Authenticator option. The Google Authenticator registration UI opens.

[56] (Optional) Click the Resend MFA button if a voice call or text message is not received after 30 seconds has elapsed.

[57] A message is displayed which indicates the MFA device was correctly added.

[58] If the user clicks the Cancel button instead of entering the one-time verification code, the respective device will remain in a Pending state. The device will need to be activated using this activation procedure.

[59] An email is sent to the user's email address of record which indicates that changes were made to the user's account and the new MFA device appears as an optional authentication factor the next time the user signs in.

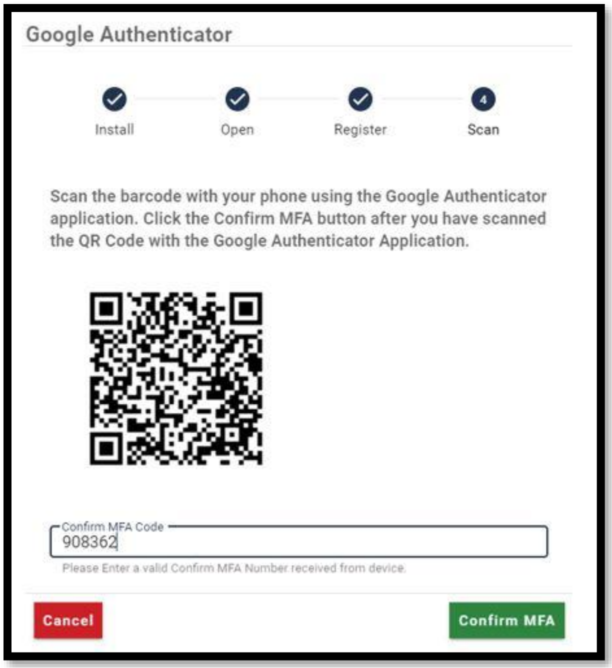


Launch your phone's application store, search for Google Authenticator and install it. If you have a CMS issued iPhone, then please download your app through the CMS App Store.

Figure 33: Google Authenticator MFA Device Registration UI

4. Click the Next button and follow the Manage MFA Devices function on-screen prompts for installing a Google Authenticator MFA device.
5. (Conditional) If it is not already installed, download, and install the Google Authenticator Chrome browser plugin from the Chrome web store. The Google Authenticator browser plugin icon appears in the top row of icons on the right side of the browser window.
6. Click the “Register Device” button on the Google Authenticator setup UI. [60]

[60] This step generates a QR code that will be used to register the browser plugin MFA device that is running on the desktop or laptop computing device as an active MFA device in the user’s profile.



Google Authenticator

Scan the barcode with your phone using the Google Authenticator application. Click the Confirm MFA button after you have scanned the QR Code with the Google Authenticator Application.

Confirm MFA Code: 908362

Please Enter a valid Confirm MFA Number received from device.

Figure 34: Google Authenticator MFA Device Registration Quick Response (QR) Code.

7. Click the Google Authenticator browser plugin icon. The Authenticator plugin activates and displays the UI shown in *Figure 35: Google Authenticator Browser Plugin with Scan/Action Button*.

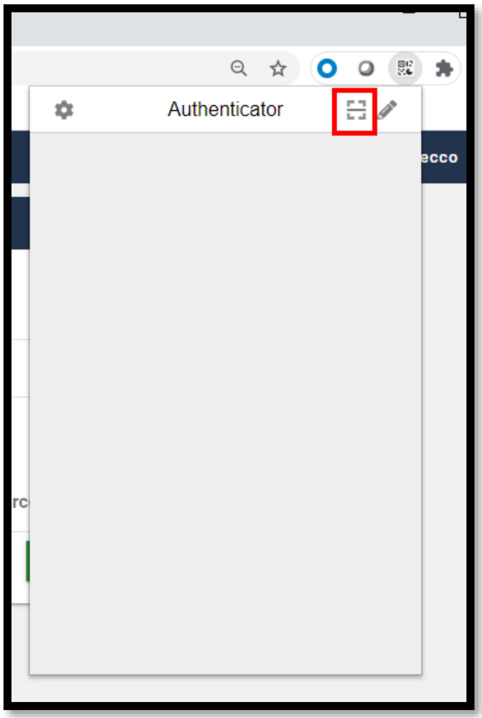
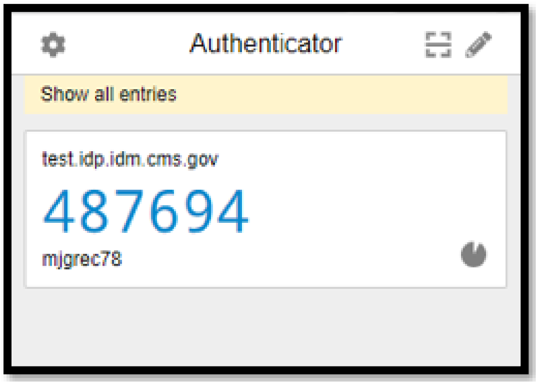


Figure 35: Google Authenticator Browser Plugin with Scan/Action Button

8. Click the Scan/Action button on the Google Authenticator browser plugin. A QR code appears.

9. Position the mouse pointer just outside the top left corner of the QR code, then click and drag the mouse pointer around the boundary of the QR code then release it. [61]

10. Click the Scan/Action button on the Google Authenticator browser plugin. A one-time verification code appears in the Authenticator browser plugin UI.



test.idp.idm.cms.gov
487694
mjgrec78

Figure 36: Google Authenticator Browser Plugin with One-time Verification Code

11. Enter the one-time verification code into the Confirm MFA Code field and click the Confirm MFA button.

12. A message appears, indicating that the MFA device was correctly added. Click the OK button. [62]

9.8.5 How to Add a Google Authenticator Mobile App 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 allows the user to receive one-time verification codes even when the user does not have an internet connection or mobile service.

This section provides the steps that users must follow to add a Google Authenticator mobile app MFA device to the user's account.

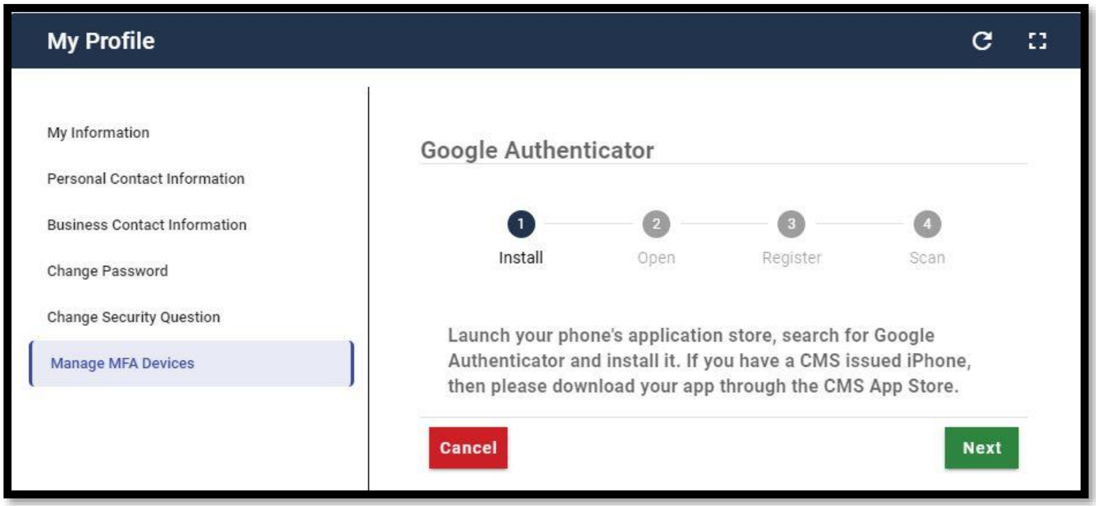
1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.

2. Click the Manage MFA Devices link. The Manage MFA Devices function opens.

3. Click the Add another device drop-down menu and select the Google Authenticator option. The Google Authenticator registration UI opens.

[61] If the QR code is recognized, a small window appears and display a message that indicates the operation was successful.

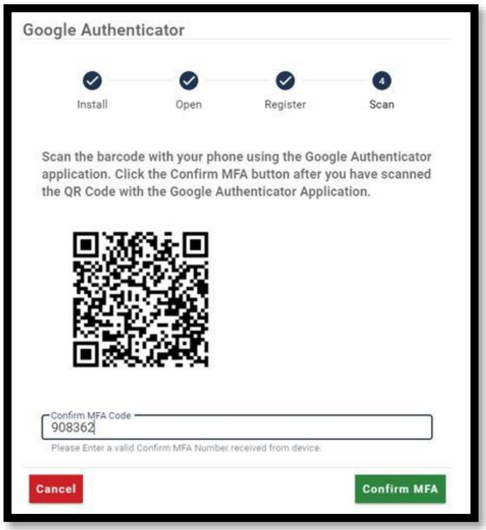
[62] An email is sent to the user's email address of record which indicates that an MFA device has been added to the account and the new device appears as an optional authentication factor the next time the user signs in.



Launch your phone's application store, search for Google Authenticator and install it. If you have a CMS issued iPhone, then please download your app through the CMS App Store.

Figure 37: Google Authenticator MFA Device Registration UI

4. Click the Next button and follow the Manage MFA Devices function on-screen prompts for installing a Google Authenticator MFA device.
5. Download and install the Google Authenticator mobile app onto the mobile device. Obtain the app from the appropriate app store. [63]
6. Click the “Register Device” button on the IDM Google Authenticator setup UI. This step generates a QR code that will be used to register the mobile device as an active MFA device in the user’s profile.



Scan the barcode with your phone using the Google Authenticator application. Click the Confirm MFA button after you have scanned the QR Code with the Google Authenticator Application.

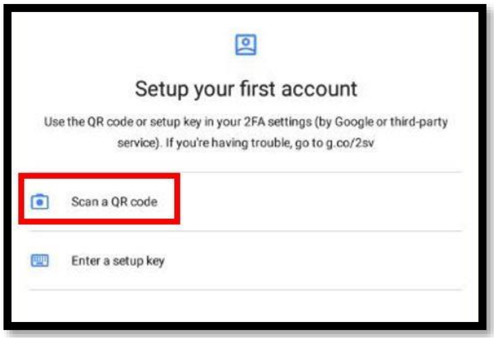
Confirm MFA Code: 908362

Please Enter a valid Confirm MFA Number received from device.

Figure 38: Google Authenticator MFA Device Registration QR Code

7. Launch the Google Authenticator app on the mobile device and click the “Get Started” button. The Account Setup screen appears.

[63] Users who access the IDM System with CMS issued mobile phones must download the Google Authenticator app through the CMS app store and may require the assistance / permission of their IT department. Users who access the IDM System with personally owned mobile phones must use their respective app stores.



Setup your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

Figure 39: Google Authenticator Mobile App Setup Screen

8. Click the Scan a QR code button on the Google Authenticator app, then Scan the QR code using the Google Authenticator mobile app. The Google Authenticator app generates a one-time verification code.
9. Type the one-time verification code into the Confirm MFA Code field and click the Confirm MFA button.
10. A message appears, indicating that the MFA device was correctly added.
11. Click the OK button. [64]

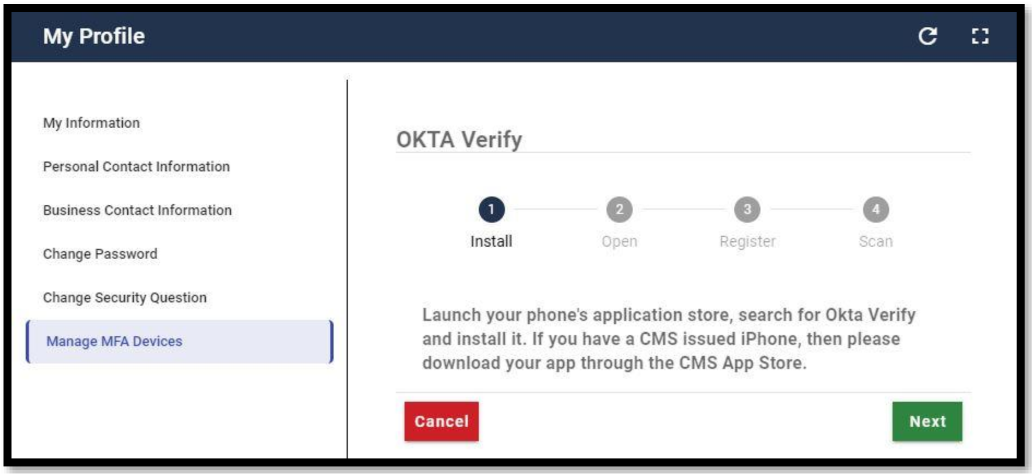
9.8.6 How to Add an Okta Verify MFA Device

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.

This section provides the steps that users must follow to add an Okta Verify MFA device to the user's account.

1. Click the My Profile button located on the Self-Service UI or Click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Manage MFA Devices link. The Manage MFA Devices function opens.
3. Click the Add another device drop-down control and select the Okta Verify option. The Okta Verify registration UI opens.

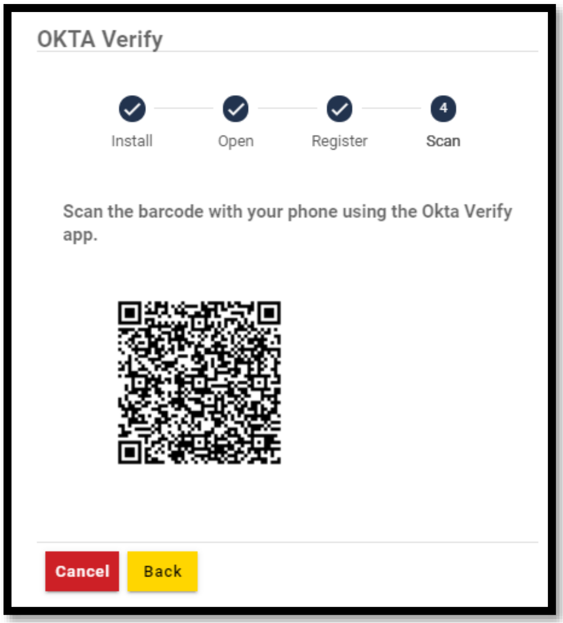
[64] An email is sent to the user's email address of record which indicates that changes were made to the user's account and the new device appears as an optional authentication factor the next time the user signs in.



Launch your phone's application store, search for Okta Verify and install it. If you have a CMS issued iPhone, then please download your app through the CMS App Store.

Figure 40: Okta Verify MFA Device Registration UI

4. Click the Next button and follow the Manage MFA Devices function on-screen prompts for installing an Okta Verify MFA device.
5. Download and install the Okta Verify app onto the mobile device. Obtain the app from the appropriate app store. [65]



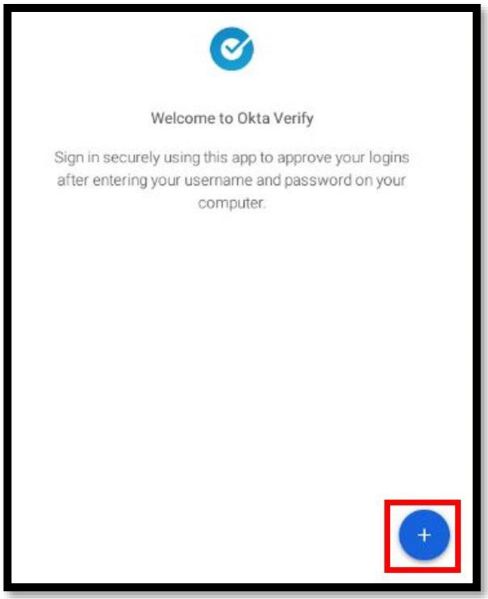
Scan the barcode with your phone using the Okta Verify app.

Figure 41: Okta Verify MFA Device Registration QR Code

6. Click the “Register Device” button on the IDM Okta Verify setup UI. This step generates a QR code that will be used to register the mobile device as an active MFA device in the user’s profile.

[65] Users who access the IDM System with CMS issued mobile phones must download the Okta Verify app through the CMS app store and may require the assistance / permission of their IT department. Users who access the IDM System with personally owned mobile phones must use their respective app stores.

7. Launch the Okta Verify app on the mobile device and click the “Get Started” button. The Account Setup screen appears.



Welcome to Okta Verify

Sign in securely using this app to approve your logins after entering your username and password on your computer.

Figure 42: Okta Verify Mobile App Setup Screen

8. Click the Add Account button on the Okta Verify mobile app, then scan the QR Code using the Okta Verify mobile app.
9. A message appears, indicating that the MFA device was correctly added. Click the OK button. [66]

9.8.7 How to Edit Email MFA Device Settings

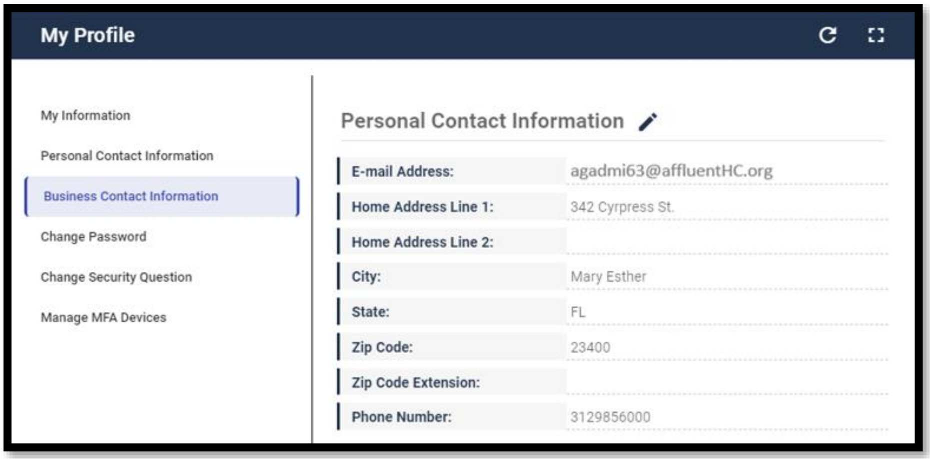
This section provides the steps that users must follow to edit their MFA device settings using the Edit Factor control. [67]

Note: The settings for IVR, SMS, Google Authenticator, and Okta MFA devices cannot be modified after they are activated. If changes are necessary, those devices must be removed using the procedure in section *9.8.8 How to Remove an MFA Device*, then re-added using the respective procedure.

1. With the Manage MFA Devices UI open, click the Edit Factor icon for the Email MFA device.

[66] An email is sent to the user’s email address of record which indicates that changes were made to the user’s account and the new device appears as an optional authentication factor the next time the user signs in.

[67] Email MFA device settings are tied directly to the user’s profile information, so changes to the Email MFA device settings will affect user profile settings.



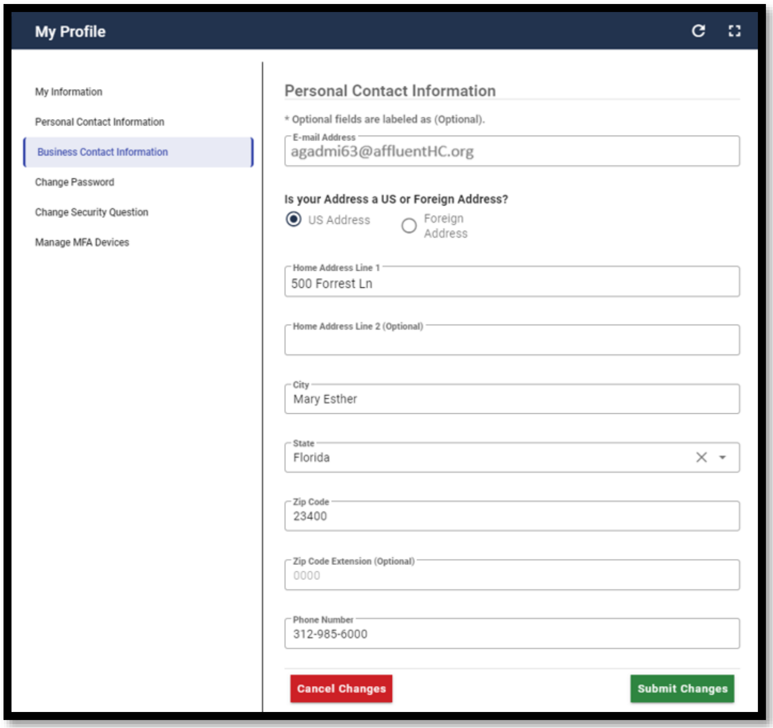
Personal Contact Information

E-mail Address:	agadmi63@affluentHC.org
Home Address Line 1:	342 Cyrpress St.
Home Address Line 2:	
City:	Mary Esther
State:	FL
Zip Code:	23400
Zip Code Extension:	
Phone Number:	3129856000

Figure 43: Edit Email MFA Device Settings (Personal Contact Information UI)

2. Click the Edit icon ✎ then enter the new email address. [68]

[68] For an Email MFA device, the user is redirected to the My Profile - Personal Contact Information form to change their email address.



Personal Contact Information

* Optional fields are labeled as (Optional).

E-mail Address: agadmi63@affluentHC.org

Is your Address a US or Foreign Address?

● US Address ○ Foreign Address

Home Address Line 1: 500 Forrest Ln

Home Address Line 2 (Optional):

City: Mary Esther

State: Florida

Zip Code: 23400

Zip Code Extension (Optional): 0000

Phone Number: 312-985-6000

Figure 44: Edit Email MFA Device Settings (Personal Contact Information Form)

3. Click the Submit Changes button to save the new settings. [69, 70]

9.8.8 How to Remove an MFA Device

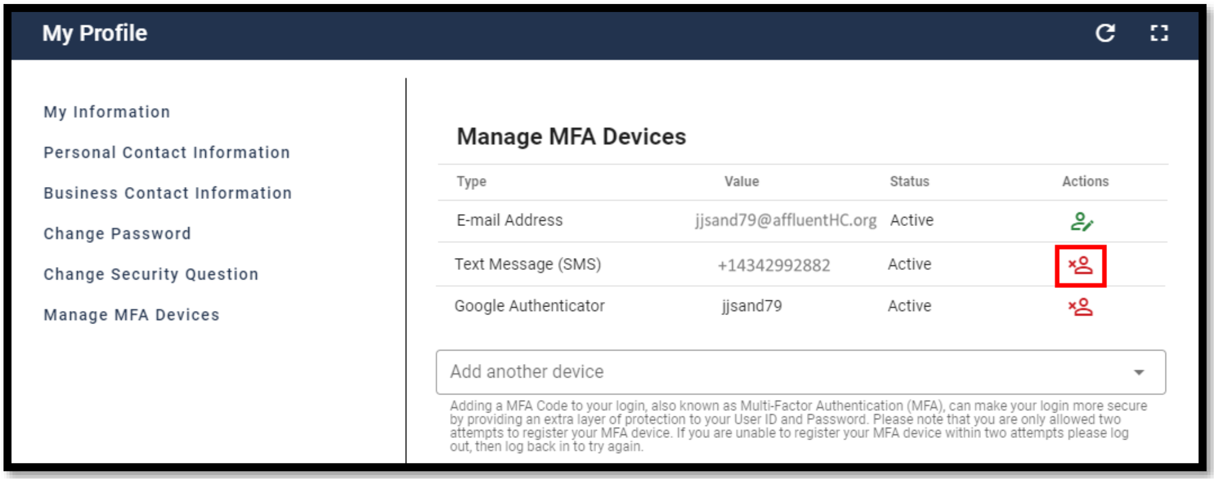
This section provides the steps that users must follow to remove an MFA device from their account using the Remove Factor control. [71]

1. Click the My Profile button located on the Self-Service UI or click the My Profile taskbar option. These controls are shown in *Figure 18: My Profile Button and My Profile Taskbar Option*.
2. Click the Manage MFA Devices link. The Manage MFA Devices function opens.

[69] Click the Cancel Changes button to discard the changes and keep the original setting.

[70] An email is sent to the user's old and new email address which indicates that changes were made to the user's account.

[71] The Email MFA device cannot be removed by the user.



My Profile

Manage MFA Devices

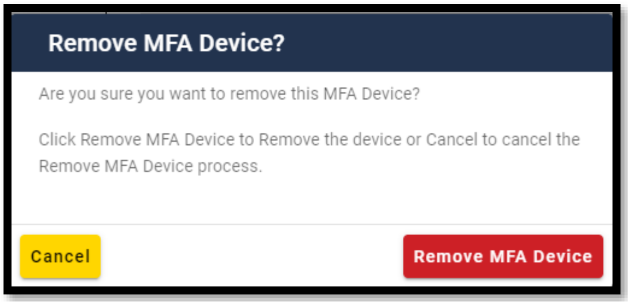
Type	Value	Status	Actions
E-mail Address	jjsand79@affluentHC.org	Active	✎
Text Message (SMS)	+14342992882	Active	✕
Google Authenticator	jjsand79	Active	✕

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 45: Manage MFA Devices Function - Remove Factor

3. Click the Remove Factor icon for the MFA device that requires removal. The Remove MFA Device decision UI appears.



Remove MFA Device?

Are you sure you want to remove this MFA Device?

Click Remove MFA Device to Remove the device or Cancel to cancel the Remove MFA Device process.

Figure 46: Remove MFA Device Decision UI

4. Click the Remove MFA Device button. [72, 73]

[72] An email is sent to the user's email address of record which indicates that changes were made to the user's account. The MFA device no longer appears in the Manage MFA Devices window, and it no longer appears as an authentication option for system sign-in.

[73] (Optional) Click the Cancel button to abort the Remove MFA Device action. The MFA device will remain in its current state.

10. How to Use the IDM Manage My Roles Function

Users can view and manage assigned roles by using the **Manage My Roles** button located on the Self-Service UI or the Manage My Roles taskbar option.

The **Manage My Roles** function enables users to perform role management tasks for applications to which they currently have access. Users may perform the following tasks:

- View a summary of current roles
- View role details
- Modify a role
- Add a role
- Remove a role

10.1 How to Launch and Close the Manage My Roles Function

Launch the Manage My Roles Function:

1. Click the Manage My Roles button located on the Self-Service UI or Click the Manage My Roles taskbar option.

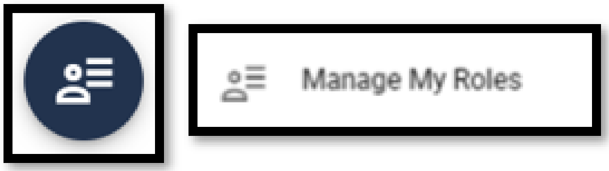


Figure 47: Manage My Roles Function Button and Taskbar Option

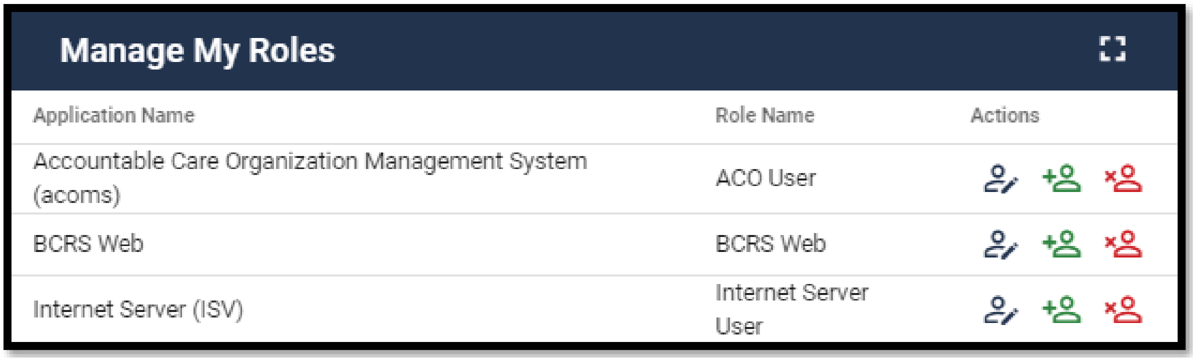
Close the Manage My Roles Function:

1. Choose one of the following actions to close the Manage My Roles function:
    - Click the IDM Self-Service button located at the top left of the Self-Service UI.
    - Select another function from the Self-Service taskbar.
    - Select the Log Out option from the drop-down menu and log out of the system.

10.2 How to View a Summary of Approved Roles

This section provides the steps that users must follow to view a summary of their approved roles.

1. Click the Manage My Roles button located on the Self-Service Dashboard or click the Manage My Roles taskbar option. These controls are shown in *Figure 47: Manage My Roles Function Button and Taskbar Option*.



Manage My Roles

Application Name	Role Name	Actions
Accountable Care Organization Management System (acoms)	ACO User	👤✎ +👤 ×👤
BCRS Web	BCRS Web	👤✎ +👤 ×👤
Internet Server (ISV)	Internet Server User	👤✎ +👤 ×👤

Figure 48: Manage My Roles UI

The Manage My Roles UI displays the list of the logged in users currently assigned roles listed by application name and displays the following information for each role:

- Application Name
- Role Name
- Role attribute information [74, 75, 76]

Table 9: Manage My Roles Function Controls describes the controls that are used by the My Roles Function. These controls are used in addition to the common controls listed in *Table 5: Self-Service UI Common Controls*.

Table 9: Manage My Roles Function Controls

Control Name	Icon	Function
View/Edit Details	👤✎	This control opens the Application Roles UI to display role details for the selected application.
Add Role	+👤	This control is used to submit a request to add a new role to the selected application.
Remove Role	×👤	This control is used to submit a request to remove a role from the selected application.

10.3 How to View Role Details

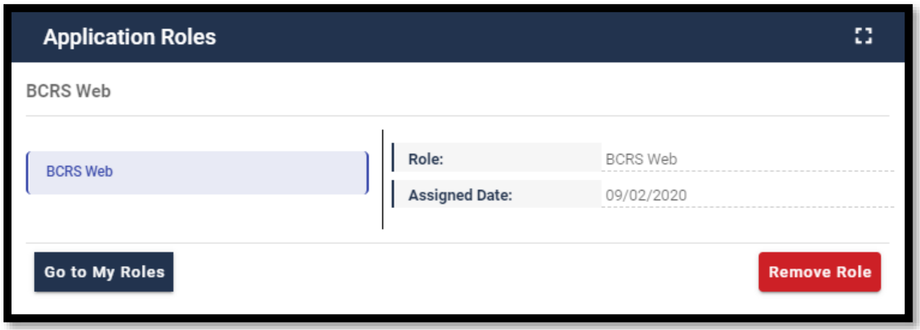
This section provides the procedure that is used to view the details of a selected role using the Application Roles UI.

[74] Role attributes fall into the broad categories of Routing, Decision, or Organization.

[75] Not every application has role attributes. Role attributes are specific to each role. Role attributes are the only aspects of role that an end user can modify.

[76] (Optional) The user may click the column headings of the summary to change the sorting order of the displayed information.

1. Click the Manage My Roles button located on the Self-Service UI or click the Manage My Roles taskbar option. These controls are shown in *Figure 47: Manage My Roles Function Button and Taskbar Option*.
2. Click the View/Edit control that is located on the Manage My Roles UI. The Application Roles UI opens.



Application Roles

BCRS Web

Role:	BCRS Web
Assigned Date:	09/02/2020

Figure 49: Manage My Roles - Application Roles UI

The details of a selected role are displayed using the Application Roles UI. The Application Roles UI displays the following details for each role:

- Application Name
- Role Name
- Assigned Date

- Role attribute information (Conditional) [77, 78]

The Application Roles UI also provides access to the following controls that enable the currently logged in user to perform the following role management tasks:

- Remove Role button
- Modify Role button (Conditional) [79]

10.4 How to Remove a Role

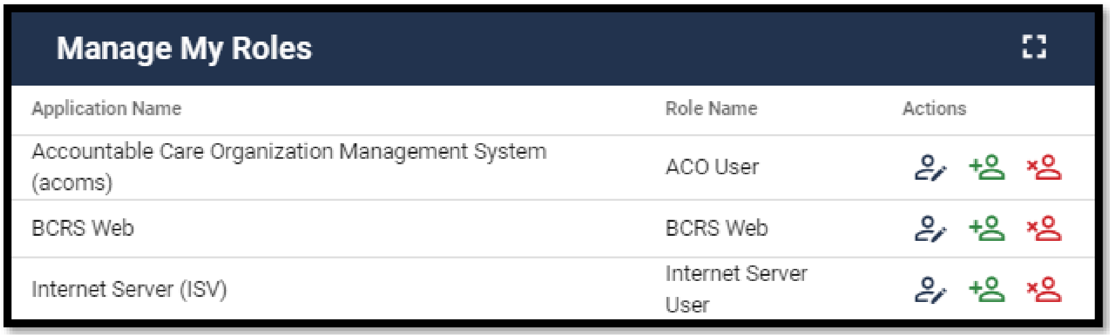
This section provides the steps that users must follow to remove a role using the Manage My Roles function. Roles may be removed using the UI controls provided on the following UIs:

- The Manage My Roles UI
- The Application Roles UI

Note: Role removal requests do not require approval and they are executed the instant that the IDM System accepts the request from the user. [80]

10.4.1 How to Remove a Role using the Manage My Roles UI

1. Click the Manage My Roles button located on the Self-Service UI or click the Manage My Roles taskbar option. These controls are shown in Figure 50: Manage My Roles UI.



Manage My Roles

Application Name	Role Name	Actions
Accountable Care Organization Management System (acoms)	ACO User	
BCRS Web	BCRS Web	
Internet Server (ISV)	Internet Server User	

Figure 50: Manage My Roles UI

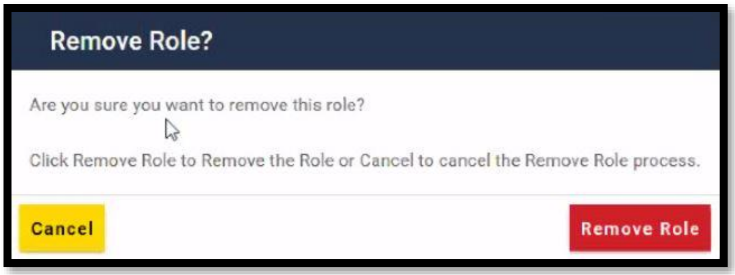
2. Click the Remove Role icon. The Remove Role decision UI opens.

[77] Not every application has role attributes. Role attributes are specific to each role. Role attributes are the only aspects of role that an end user can modify.

[78] Role attributes fall into the broad categories of Routing, Decision, or Organization.

[79] Role attributes are the only parameters that a user can modify, so the Modify Role button appears if the role details include attribute information.

[80] The removal of the last approver role associated to an Organization can leave users in an “orphaned” state without an approver of record for future role requests. The system displays a warning message if the role removal operation could affect the last approver of an organization that still has users associated with it.



Are you sure you want to remove this role?

Click Remove Role to Remove the Role or Cancel to cancel the Remove Role process.

Figure 51: The Remove Role Decision UI

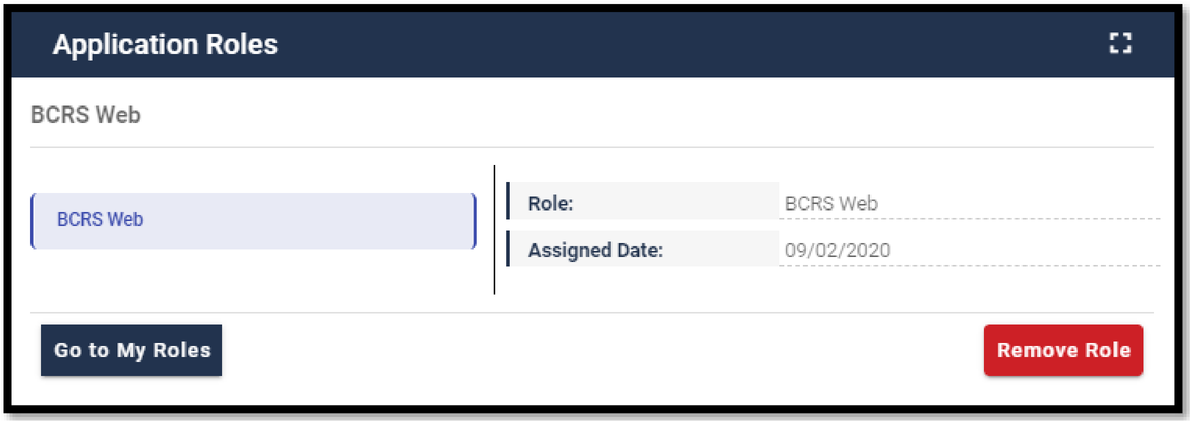
3. Click the Remove Role button. [81]

   If the role removal request was successful, the Manage My Roles UI displays Request ID information and a message that informs the user that the request was successfully submitted. [82]

4. Click the Go to My Roles button.

10.4.2 How to Remove a Role using the Application Roles UI

1. Launch the Application Roles function using the procedure described in section *10.3 How to View Role Details*.



Role: BCRS Web

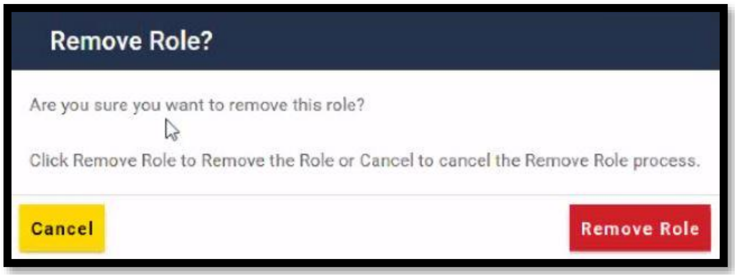
Assigned Date: 09/02/2020

Figure 52: Manage My Roles - Application Roles UI Displays Role with no Attributes

2. Click the Remove Role button. The Remove Role decision UI opens.

[81] (Optional) click the Cancel button to terminate the Remove Role operation.

[82] An email is sent to the user's email address of record which indicates that the role removal request was accepted.



Remove Role?

Are you sure you want to remove this role?

Click Remove Role to Remove the Role or Cancel to cancel the Remove Role process.

Figure 53: The Remove Role Decision UI

3. Click the Remove Role button. [83]

   If the role removal request was successful, the Application Roles UI displays Request ID information and a message that informs the user that the request was successfully submitted. [84]

4. Click the Go to My Roles button.

[83] (Optional) click the Cancel button to terminate the Remove Role operation.

[84] An email is sent to the user’s email address of record which indicates that the role removal request was accepted.

11. How to Use the IDM My Requests Function

Users can view and manage pending role and application requests by using the My Requests function button located on the Self-Service UI, the My Requests taskbar option, or the My Requests Counter icon on the Self-Service UI.

11.1 How to Launch and Close the My Requests Function

Launch the Manage My Requests Function:

1. Click the My Requests button located on the Self-Service UI, the My Requests option located on the taskbar, or the My Requests Indicator located on the Self-Service UI.

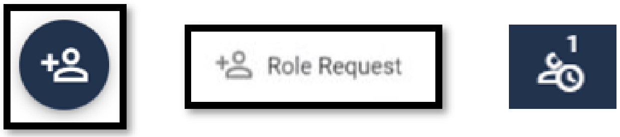


Figure 54: The My Requests Button, Taskbar Option, and Indicator

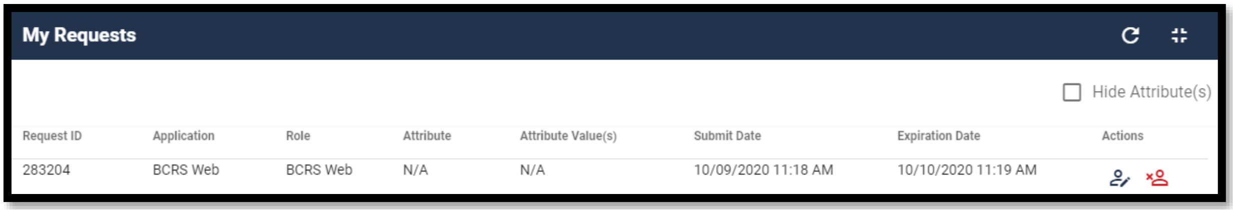
Close the My Requests Function:

1. Choose one of the following actions to close the My Requests function:
   - Click the IDM Self-Service button located at the top left corner of the Self-Service UI.
   - Select another function from the Self-Service taskbar.
   - Select the Log Out option from the dropdown menu and log out of the system.

11.2 How to View Pending Requests

This section provides the steps that users must follow to view pending requests.

1. Click the My Requests button, the My Requests taskbar option, or the My Requests indicator. These controls are shown in *Figure 54: The My Requests Button, Taskbar Option, and Indicator*.

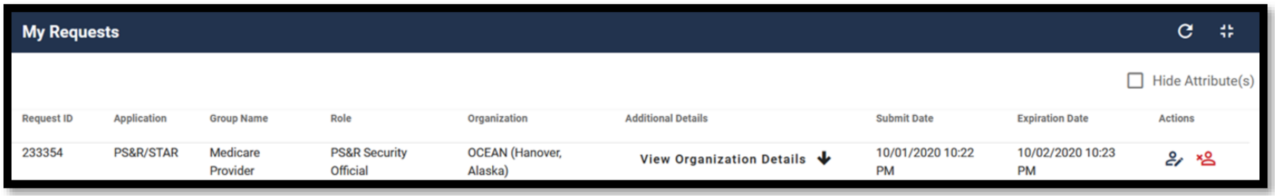


My Requests

□ Hide Attribute(s)

Request ID	Application	Role	Attribute	Attribute Value(s)	Submit Date	Expiration Date	Actions
283204	BCRS Web	BCRS Web	N/A	N/A	10/09/2020 11:18 AM	10/10/2020 11:19 AM	

Figure 55: My Requests UI Displays Role with No Attributes



My Requests

□ Hide Attribute(s)

Request ID	Application	Group Name	Role	Organization	Additional Details	Submit Date	Expiration Date	Actions
233354	PS&R/STAR	Medicare Provider	PS&R Security Official	OCEAN (Hanover, Alaska)	View Organization Details	10/01/2020 10:22 PM	10/02/2020 10:23 PM	

Figure 56: My Requests UI Displays Role with Attributes & Details

The My Requests UI displays a list of the logged in user's current requests that are pending approval action. [85]

The list contains the following information for each pending request:

- Request ID
- Application
- Role
- Role attribute and detail information (Conditional) [86, 87]
- Submit Date
- Expiration Date

Table 10: My Requests Function Controls describes the controls that are used by the My Requests function. These controls are used in addition to the common controls listed in *Table 5: Self-Service UI Common Controls*.

Table 10: My Requests Function Controls

Control Name	Icon	Function
Cancel Request		This control deletes a specific Pending Request.
View Details		This control opens the Pending Request Details UI for the selected request.

[85] (Optional) The user may click the column headings of the summary to change the sorting order of the displayed information.

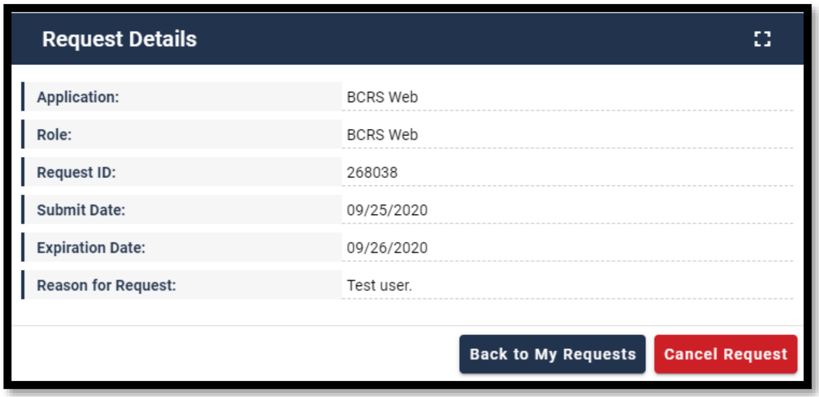
[86] Not every application has role attributes. Role attributes are specific to each role, and they are the only aspects of role that an end user can modify.

[87] Where relevant, additional role attribute detail information can be accessed using the View Details Control.

11.3 How to View Pending Request Details

This section provides the steps that users must follow to view request details using the Request Details UI.

1. Click the My Requests button, the My Requests taskbar option, or the My Requests indicator. These controls are shown in *Figure 54: The My Requests Button, Taskbar Option, and Indicator*.
2. Click the corresponding View Details icon to review the details of the desired pending request. [88, 89, 90]



Request Details

Application:	BCRS Web
Role:	BCRS Web
Request ID:	268038
Submit Date:	09/25/2020
Expiration Date:	09/26/2020
Reason for Request:	Test user.

Figure 57: Request Details UI Displays Role with no Attributes

3. Click the Back to My Requests button to close the Request Details UI and return to the My Pending Requests UI.

11.4 How to Cancel Pending Requests

The procedure in this section provides the steps that users must follow to cancel pending requests. Pending requests may be removed using the Manage My Roles Function.

This section provides the steps that users must follow to remove a role using the Manage My Roles function. Roles may be removed using the UI controls provided on the following UIs:

- My Requests UI
- The Request Details UI

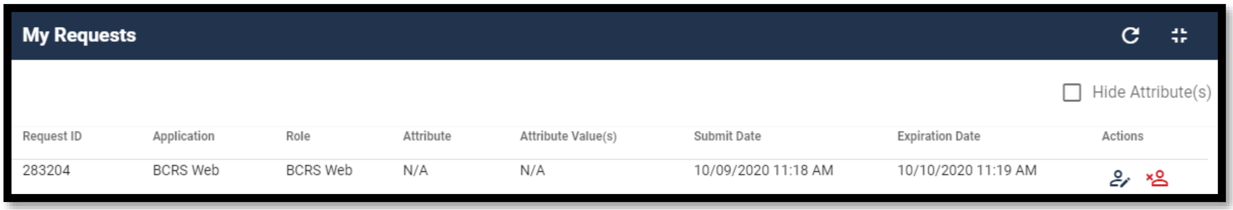
[88] The Request Details window also provides access to the Cancel Request function that enables the user to cancel that specific pending request.

[89] Pending Request detail information categories include Application, Role, Request ID, Submit Date, Expiration Date, Reason for Request, and Role Attributes (Conditional).

[90] Not every application has Role Attributes. Role Attributes are specific to each role. Role Attributes are the only aspects of role that an end user can modify.

11.4.1 How to Cancel a Pending Request Using the My Requests UI

1. Click the My Requests button, the My Requests taskbar option, or the My Requests indicator. These controls are shown in *Figure 54: The My Requests Button, Taskbar Option, and Indicator*.

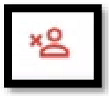


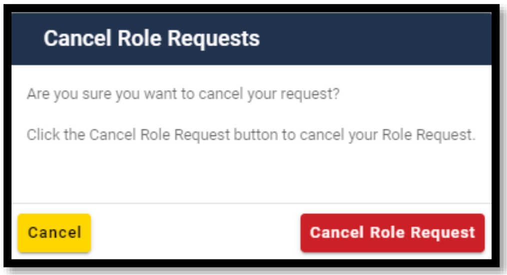
My Requests

□ Hide Attribute(s)

Request ID	Application	Role	Attribute	Attribute Value(s)	Submit Date	Expiration Date	Actions
283204	BCRS Web	BCRS Web	N/A	N/A	10/09/2020 11:18 AM	10/10/2020 11:19 AM	

Figure 58: My Requests UI Displays Role with no Attributes

2. Click the corresponding Cancel Request icon.  The Cancel Role Requests decision UI opens.



Cancel Role Requests

Are you sure you want to cancel your request?

Click the Cancel Role Request button to cancel your Role Request.

Figure 59: Cancel Role Requests Decision UI

3. Click the Cancel Role Request button. [91]

   If the cancel role request was successful, the My Requests UI displays a message that informs the user that the pending request was successfully cancelled. [92, 93]

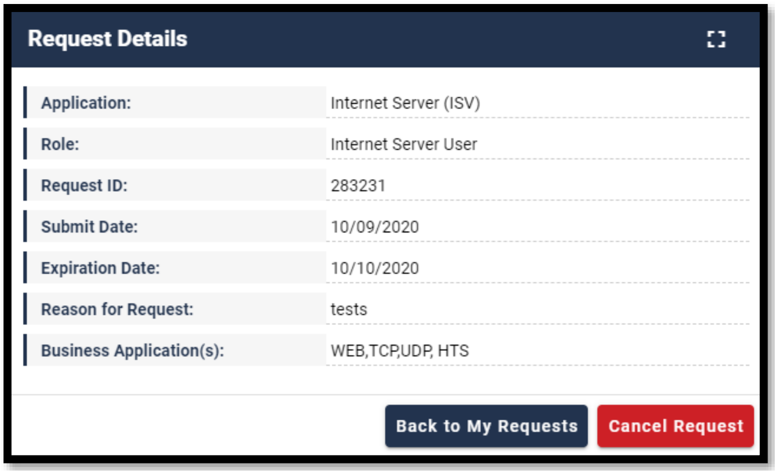
11.4.2 How to Cancel a Pending Request using the Request Details UI

1. Launch the Application Roles function using the procedure described in section *10.3 How to View Role Details*.

[91] (Optional) click the Cancel button to terminate the Cancel Role Request operation.

[92] An email is sent to the user's email address of record which indicates that the pending request cancellation request was accepted.

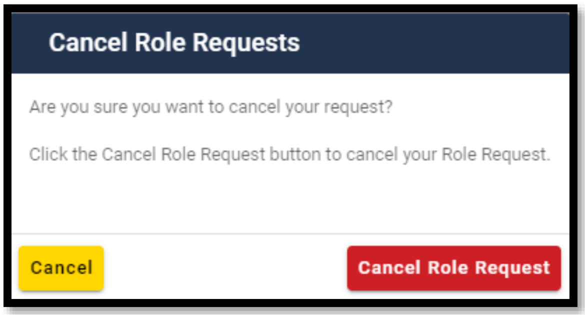
[93] The My Requests indicator on the Self-Service dashboard decreases by 1 for each pending request that is cancelled.



Application:	Internet Server (ISV)
Role:	Internet Server User
Request ID:	283231
Submit Date:	10/09/2020
Expiration Date:	10/10/2020
Reason for Request:	tests
Business Application(s):	WEB,TCP,UDP, HTS

Figure 60: Request Details UI Displays a Request for Role with Attributes

2. Click the Cancel Request button. The Cancel Role Requests decision UI opens.



Are you sure you want to cancel your request?

Click the Cancel Role Request button to cancel your Role Request.

Figure 61: Cancel Role Requests Decision UI

3. Click the Cancel Role Request button. [94]
4. If the cancel role request was successful, the My Requests UI displays a message that informs the user that the pending request was successfully cancelled. [95, 96]

[94] (Optional) click the Cancel button to terminate the Cancel Role Request operation.

[95] An email is sent to the user's email address of record which indicates that the pending request cancellation request was accepted.

[96] The My Requests indicator on the Self-Service dashboard decreases by 1 for each pending request that is cancelled.

12. How to Request HDT Access Via IDM

New HDT Users can request access to the application (and an appropriate role) by using the Role Request button located on the Self-Service UI or the Role Request taskbar option.

Note: The Role Request function is used to request access to a new application and a role when the user does not currently have a role in the application.

HDT Role Requests consist of the following steps:

1. The user selects the HDT application.
2. The user selects an appropriate HDT role.
3. The user provides a justification.
4. The user reviews and submits the request.
5. The user completes the Remote Identity Proofing (RIDP) process. [97]

12.1 How to Request Access and Role to the HDT Application

This section provides the steps that users must follow to request HDT access with the appropriate role.

1. Click the Role Request button located on the Self-Service UI or click the Role Request taskbar option. The Role Request UI appears. [98, 99]

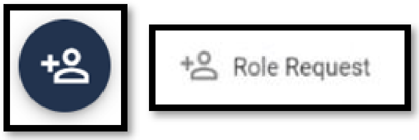


Figure 62: Role Request Button and Role Request Taskbar Option

2. Use the Select Application drop-down menu to select an Application. [100]
3. Use the Select Application drop-down menu to select an Application. Enter “HDT” and you will have an option to select the HDT application. [101]

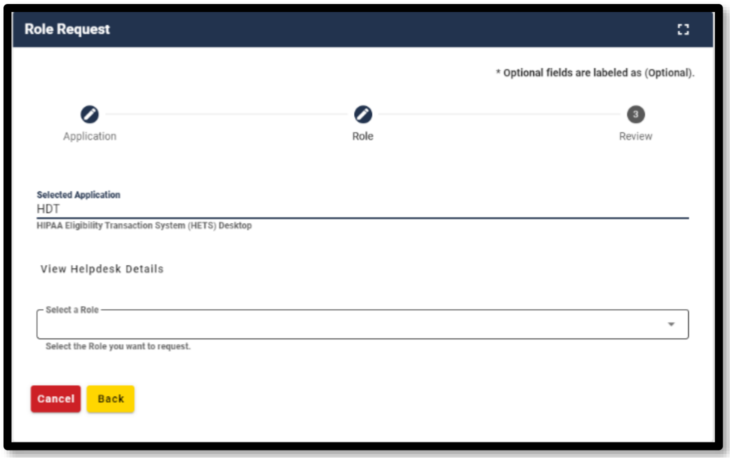
[97] RIDP is explained in section *13 Remote Identity Proofing*.

[98] The Role Request UI provides prompts and screen tips that guide the user through each step to assist users with entering information in the proper syntax and/or format.

[99] The prompts for conditional information such as RIDP depend on the role that is being requested, hence they may not appear until a role is selected.

[100] The Select Application dropdown menu will display all applications unless the user already has a role in that application.

[101] The Select Application drop-down menu will display all applications unless the user already has a role in that application.

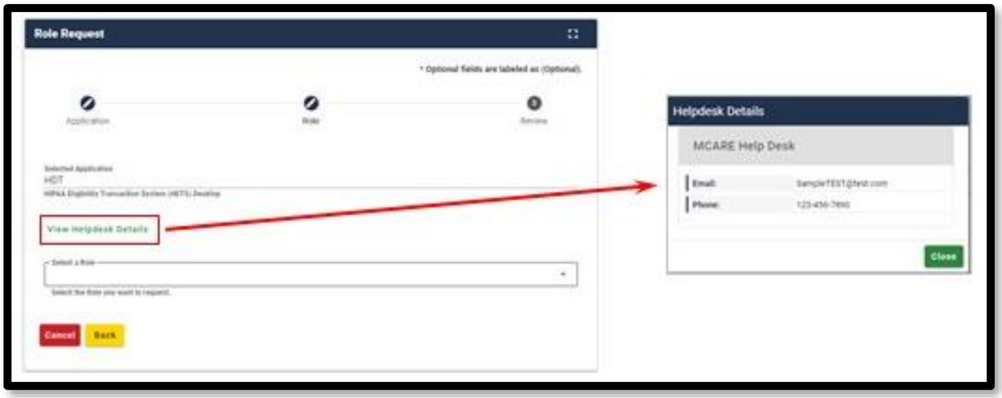


Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Select a Role
Select the Role you want to request.

Figure 63: Role Request that Requires Application and Role

4. (Optional) Click the View Helpdesk Details button to display the Application Helpdesk Details UI. [102]


Role Request
* Optional fields are labeled as (Optional).
Application
Role
Review
Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop
View Helpdesk Details
Select a Role
Select the Role you want to request.
Cancel
Back
Helpdesk Details
Close

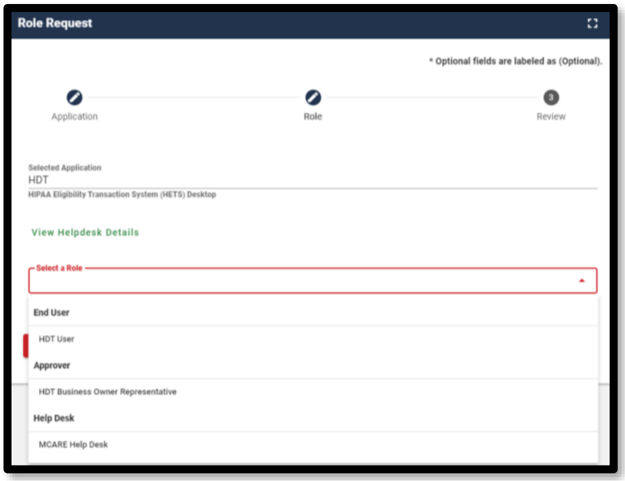
MCARE Help Desk

Email: SampleTEST@test.com
Phone: 123-456-7890

Figure 64: Role Request Helpdesk Details (Optional Step)

5. Use the Role drop-down menu to select a Role. The majority of HDT Users should choose the “End User” “HDT User” role.

[102] The Application Helpdesk may need to be contacted if there are problems with the role request. Click the Close button to hide the Helpdesk Details window.



* Optional fields are labeled as (Optional).

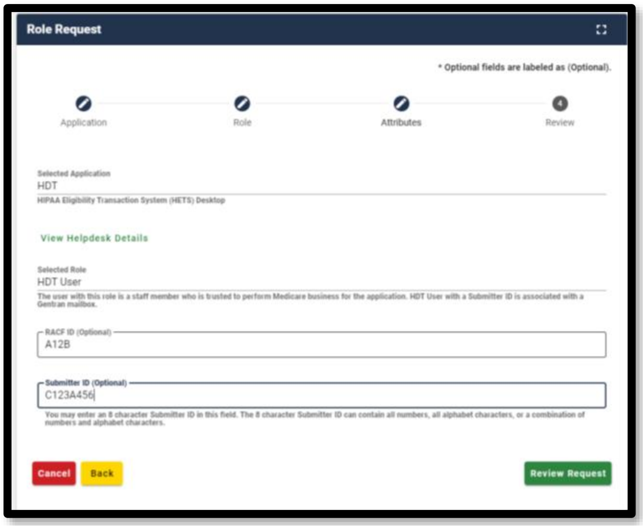
Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Select a Role

End User
HDT User
Approver
HDT Business Owner Representative
Help Desk
MCARE Help Desk

Figure 65: Role Request Specifying HDT Role

6. Enter the User's CMS RACF ID and HETS 270/271 Submitter ID information as necessary as shown in Figure 66: Role Request Specifying Additional Details.



* Optional fields are labeled as (Optional).

Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Selected Role
HDT User
The user with this role is a staff member who is trusted to perform Medicare business for the application. HDT User with a Submitter ID is associated with a Gentran mailbox.

RACF ID (Optional)
A12B

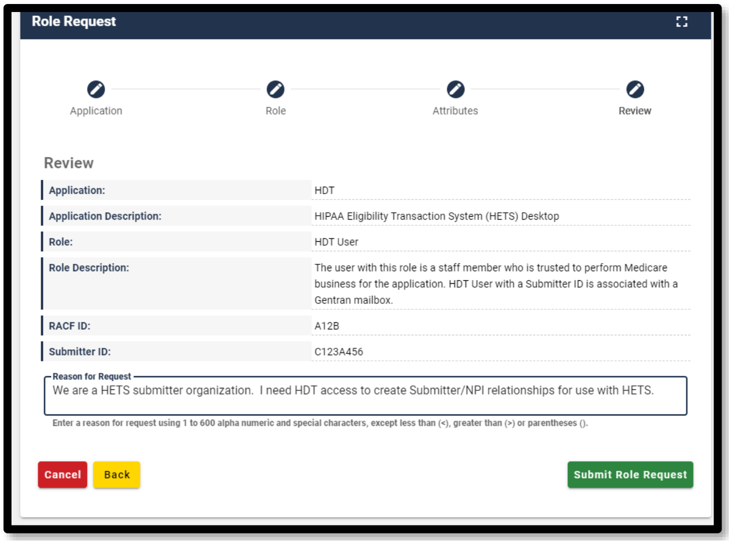
Submitter ID (Optional)
C123A456

You may enter an 8 character Submitter ID in this field. The 8 character Submitter ID can contain all numbers, all alphabet characters, or a combination of numbers and alphabet characters.

Figure 66: Role Request Specifying Additional Details

7. Click the Review Request button.

8. The screen will update to include a freeform text box titled "Reason for Request." Enter a brief justification statement into this field to provide a justification for the role request.



Review

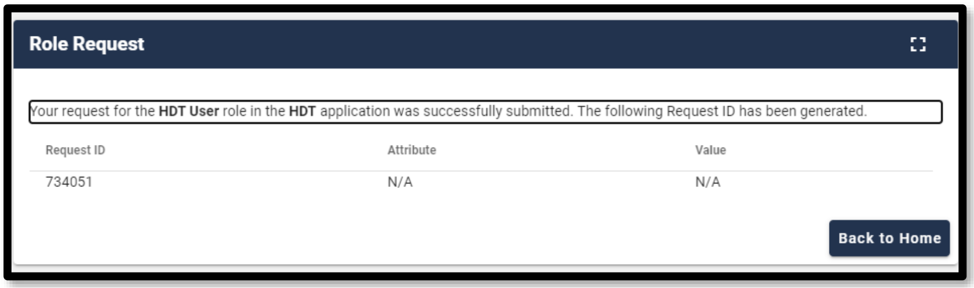
Application:	HDT
Application Description:	HIPAA Eligibility Transaction System (HETS) Desktop
Role:	HDT User
Role Description:	The user with this role is a staff member who is trusted to perform Medicare business for the application. HDT User with a Submitter ID is associated with a Gentran mailbox.
RACF ID:	A12B
Submitter ID:	C123A456

Reason for Request: We are a HETS submitter organization. I need HDT access to create Submitter/NPI relationships for use with HETS.

Enter a reason for request using 1 to 600 alpha numeric and special characters, except less than (<), greater than (>) or parentheses ().

Figure 67: Role Request Ready for Submission

9. Click the Submit Role Request button. [103, 104]



Your request for the **HDT User** role in the **HDT** application was successfully submitted. The following Request ID has been generated.

Request ID	Attribute	Value
734051	N/A	N/A

Figure 68: Successful Role Request Message

10. The Role Request UI displays a Request ID and a message that informs the user that the request was successfully submitted. [105]

11. The My Requests indicator on the Self-Service UI increments to display the user's current number of pending requests.

12. Click the Back to Home button to return to the Self-Service UI.

In addition to sending the user an email that indicates the user's request was submitted, the IDM System also sends the user subsequent emails related to the status of each request as follows:

[103] The role request is forwarded to the user's approver of record. Note that some applications may require approval by multiple approvers.

[104] Click the Back button to remain in the Role Request form and make changes or click the Cancel link to terminate the Role request process and reset the Role Request form.

[105] An email is sent to the user's email address of record which indicates that the role request was successfully submitted.

- **Approve –** The system sends an email to the user’s address on record which indicates that the request was approved. It also indicates where the user can obtain assistance if they have questions.
- **Reject –** The system sends an email to the user’s address on record which indicates that the request was rejected. It also indicates where the user can obtain assistance if they have questions.
- **Expire –** The system sends an email to the user’s address on record which indicates that the request expired due to no action taken by an approver. It also indicates where the user can obtain assistance if they have questions.

13. Remote Identity Proofing

13.1 Overview of Remote Identity Proofing (RIDP)

RIDP is an important component of the CMS IDM System. All HDT users are required to complete RIDP.

RIDP makes use of a web service and data provided by Experian, a consumer credit reporting company. Experian uses information from a user's credit history to remotely confirm the user's identity by requiring them to answer questions related to their personal credit history.

Note: Users whose home address is located outside of the United States cannot use RIDP. Those users must contact the MCARE Help Desk. For more information, refer to section *17.3 Support Information*.

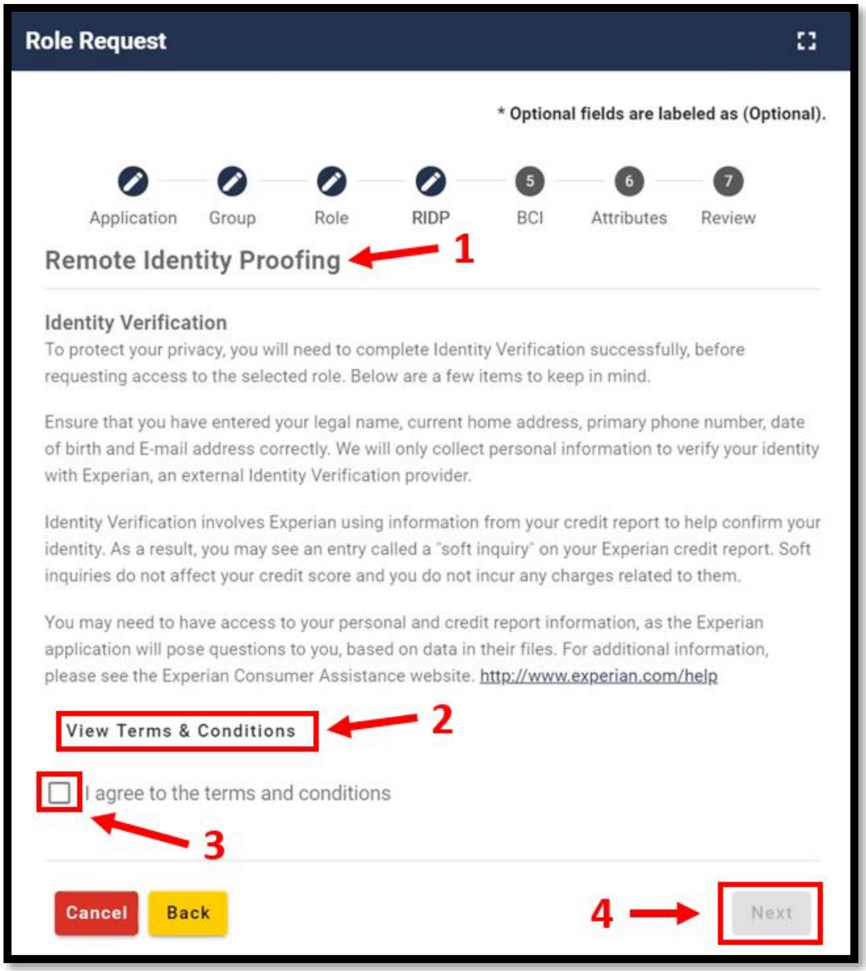
Remote Identity Proofing is a process that permits a user to verify their identity quickly using a highly reliable computer-based automated service.

Remote identity proofing consists of the following stages:

1. Review and accept the RIDP Terms and Conditions.
2. Verify user identity information.
3. Answer the Identity Proofing Questions.

13.2 Review and Accept the RIDP Terms and Conditions

After users request the HDT role, the initial page appears. This provides an overview of the RIDP process and provides users with an opportunity to review the RIDP terms and conditions. This section provides the steps to review and accept the RIDP terms and conditions.



* Optional fields are labeled as (Optional).

Remote Identity Proofing

Identity Verification

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.

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.

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.

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

View Terms & Conditions

☐ I agree to the terms and conditions

Figure 69: RIDP Overview Page with Link to Terms and Conditions

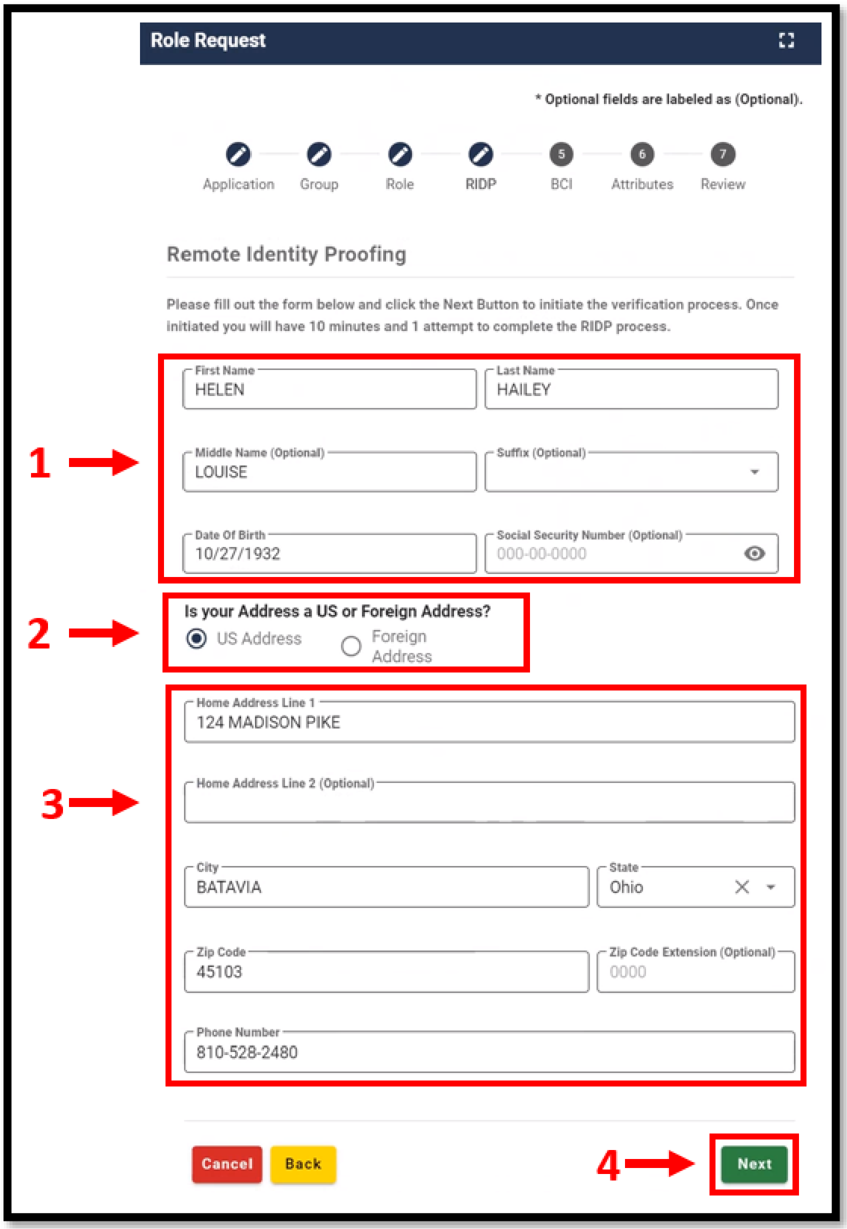
1. Review the Identity Verification description statement.
2. Click the “View Terms & Conditions” link and review the RIDP terms and conditions.
3. Click the Back button after reviewing the information.
4. Click the “I agree to the terms and conditions” check box to acknowledge agreement with the terms and conditions.
5. Click the Next button. [106]

13.3 Verify User Identity Information

This stage of the RIDP process verifies the user’s identity based on the information that they provide using this form.

[106] The Next button will not become selectable until agreement with the terms and conditions has been acknowledged.

This section provides the steps users must follow to fill out the identity verification form. [107, 108]



Role Request

* Optional fields are labeled as (Optional).

Remote Identity Proofing

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.

First Name: HELEN
Last Name: HAILEY
Middle Name (Optional): LOUISE
Suffix (Optional):
Date Of Birth: 10/27/1932
Social Security Number (Optional): 000-00-0000

Is your Address a US or Foreign Address?
● US Address ○ Foreign Address

Home Address Line 1: 124 MADISON PIKE
Home Address Line 2 (Optional):
City: BATAVIA
State: Ohio
Zip Code: 45103
Zip Code Extension (Optional): 0000
Phone Number: 810-528-2480

Figure 70: Identity Information Verification Form

1. Enter the Name, Date of Birth, and Email Address information into the respective fields. Enter the SSN into the Social Security Number field if it is required. [109]

[107] Once this form is accessed, users only have 10 minutes and 1 attempt to complete the RIDP process using this form.

[108] Some of this information was pre-populated with information from the user's profile. Pre-populated information should be reviewed to ensure that it is accurate.

[109] Under current guidelines, some roles require the user to provide a social security number (SSN) for RIDP, and others do not. For this reason, the SSN is not an optional parameter in all cases.

2. If the home address is located inside the US, keep the default “US Address” setting and proceed to the next step. [110]
3. Enter the Home Address information and the Phone Number information into the respective fields. [111]
4. Click the Next button. The Remote Identity Proofing Question page appears, and the user must respond to the questions as per the procedure in section *13.4 Answer the Remote Identity Proofing Questions*. [112, 113]

13.4 Answer the Remote Identity Proofing Questions

The remote identity proofing questions are developed by Experian and are tailored specifically to each user based on information that has been extracted from their credit report which Experian maintains in their files. This section provides the steps that must be performed to answer the identity proofing questions.

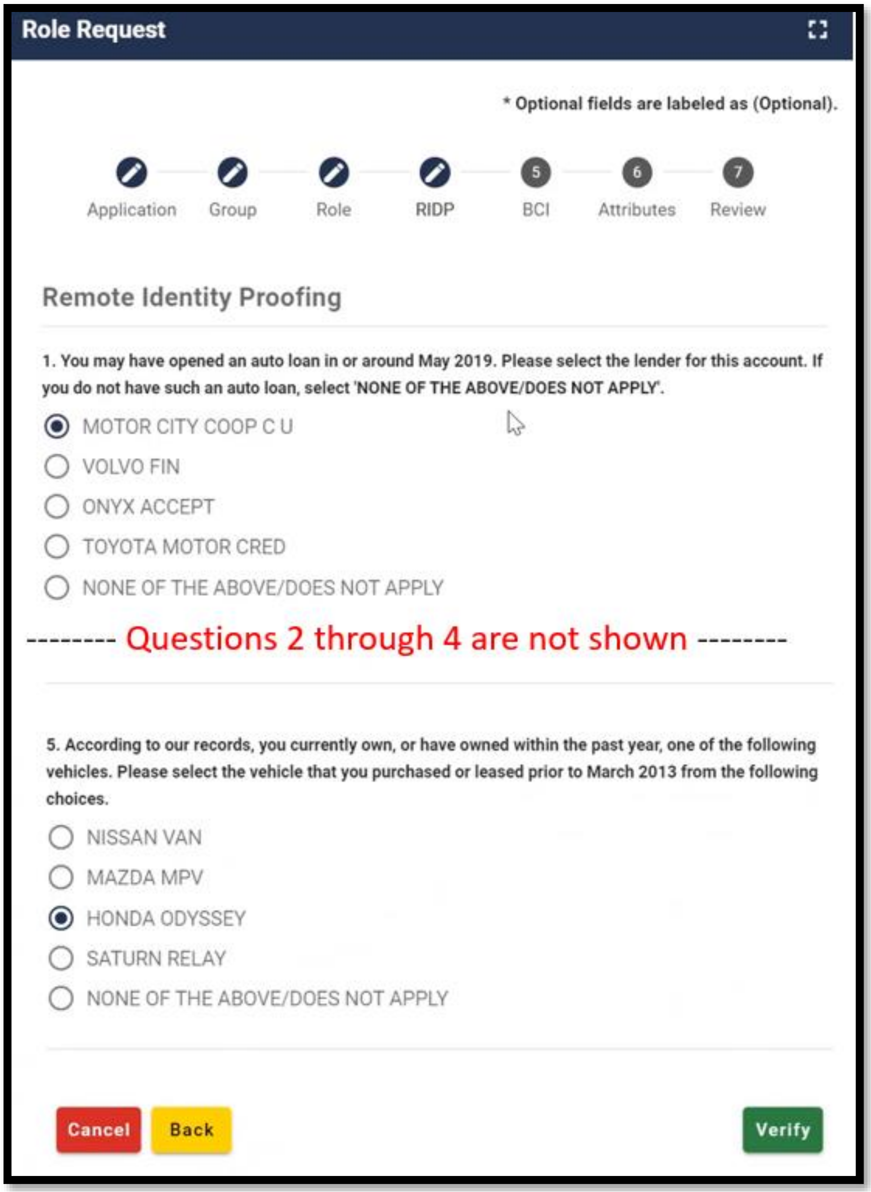
Note: A correct response must be provided for each question to successfully complete the RIDP process. A single incorrect response will cause the process to fail.

[110] If the home address is a Foreign Address, the RIDP process will fail. The user must click Cancel and terminate RIDP.

[111] The phone number must be registered to the user who is currently navigating the RIDP workflow.

[112] The Next button will not become selectable until a response is provided to all the mandatory fields on the form.

[113] If an error occurs at this stage, the user should carefully review the error message and make note of the Response Code or the Review Reference Number. Depending on the nature of the error, the message will prompt the user to contact their Application Helpdesk and provide the Response Code or contact Experian and provide the Review Reference Number.



Role Request

* Optional fields are labeled as (Optional).

Remote Identity Proofing

1. You may have opened an auto loan in or around May 2019. Please select the lender for this account. If you do not have such an auto loan, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

● MOTOR CITY COOP C U
○ VOLVO FIN
○ ONYX ACCEPT
○ TOYOTA MOTOR CRED
○ NONE OF THE ABOVE/DOES NOT APPLY

-------- Questions 2 through 4 are not shown --------

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.

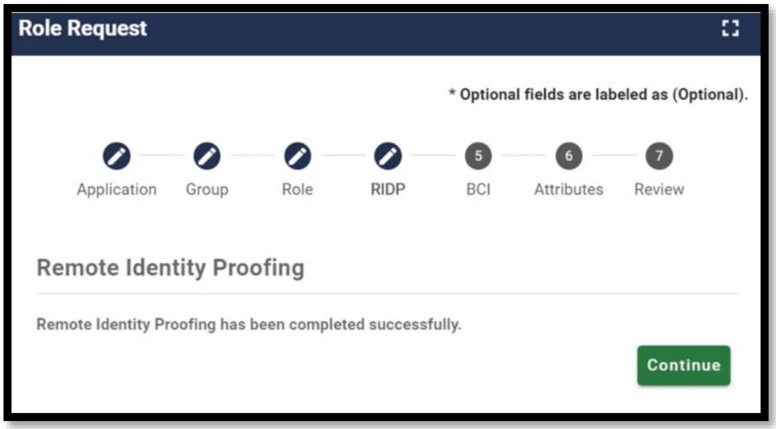
○ NISSAN VAN
○ MAZDA MPV
● HONDA ODYSSEY
○ SATURN RELAY
○ NONE OF THE ABOVE/DOES NOT APPLY

Figure 71: RIDP Proofing Questions

1. Carefully read each question and click the radio button for the most correct response to the question.
2. Click the Verify button. [114, 115]
3. The system displays a message which indicates that the RIDP process was successful.

[114] The Verify button will not become enabled until a response has been selected for all five questions.

[115] If an error occurs at this stage, proceed to section *13.4.1 How to Address RIDP Failure*.



Remote Identity Proofing

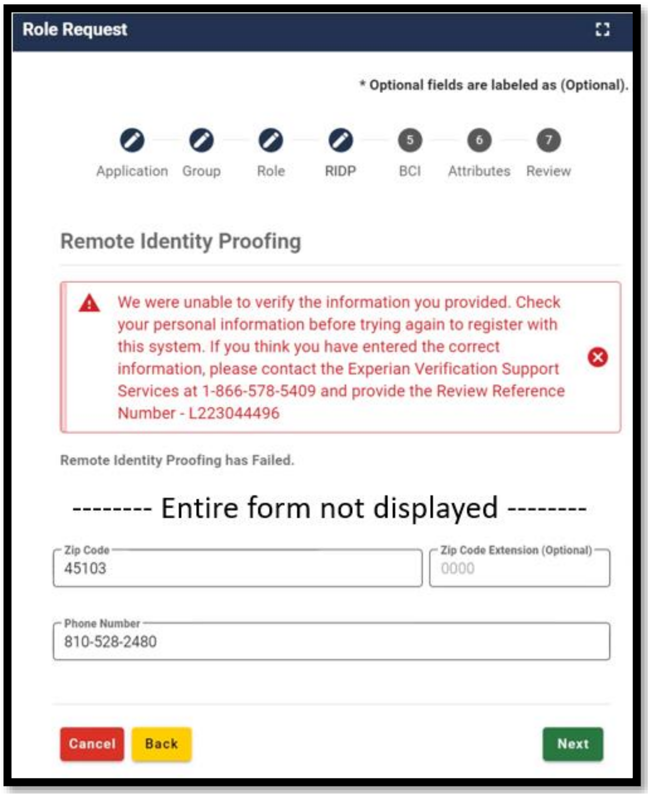
Remote Identity Proofing has been completed successfully.

Figure 72: RIDP Successful Message

4. Click the Continue button. The user is returned to the role request UI to complete the role request procedure.

13.4.1 How to Address RIDP Failure

If the RIDP process is unsuccessful, then the system displays an error message as illustrated by Figure 73: Role Request UI with RIDP Failure Message.



Remote Identity Proofing

We were unable to verify the information you provided. Check your personal information before trying again to register with this system. If you think you have entered the correct information, please contact the Experian Verification Support Services at 1-866-578-5409 and provide the Review Reference Number - L223044496

Remote Identity Proofing has Failed.

-------- Entire form not displayed --------

Zip Code: 45103

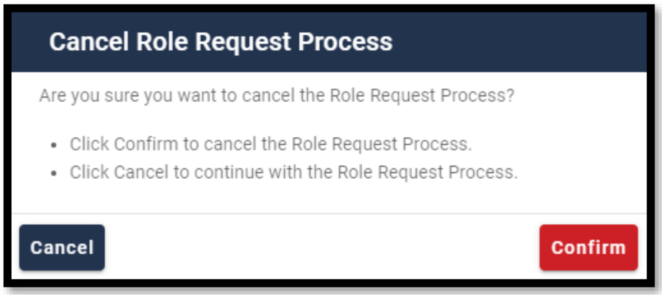
Zip Code Extension (Optional): 0000

Phone Number: 810-528-2480

Figure 73: Role Request UI with RIDP Failure Message

1. Write down the error message, contact information, and the Review Reference Number that is displayed.

2. Click the Cancel button. The Cancel Role Request Process UI appears.



Cancel Role Request Process

Are you sure you want to cancel the Role Request Process?

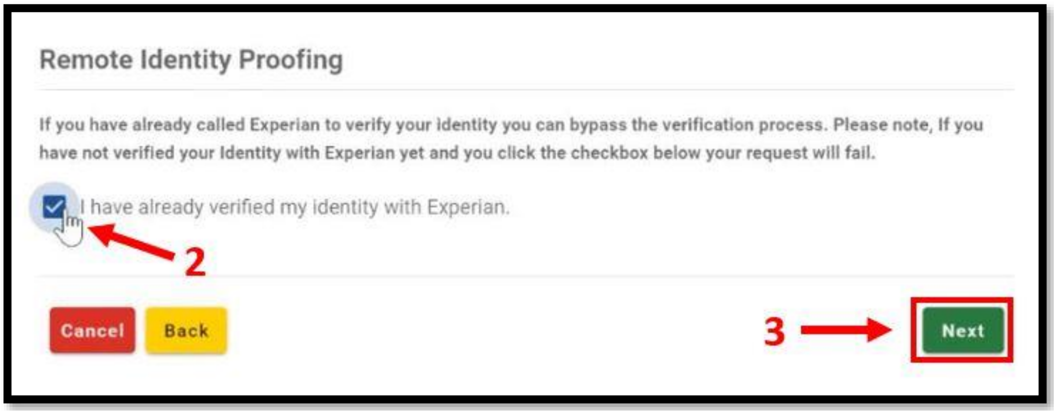
- Click Confirm to cancel the Role Request Process.
- Click Cancel to continue with the Role Request Process.

Figure 74: Cancel Role Request Process Decision Window

3. Click the Confirm button.
4. Contact Experian using the contact information provided in the error message to perform Phone Proofing. [116, 117]
5. Follow the procedure outlined in section *13.5 How to Recover from a Failed RIDP Procedure* after the Phone Proofing procedure is completed with Experian.

13.5 How to Recover from a Failed RIDP Procedure

This section provides instructions that users must follow if the online RIDP procedure fails.



Remote Identity Proofing

If you have already called Experian to verify your identity you can bypass the verification process. Please note, If you have not verified your Identity with Experian yet and you click the checkbox below your request will fail.

☑ I have already verified my identity with Experian.

Figure 75: Experian Identity Verification Confirmation

1. After performing Phone Proofing, sign in to the CMS IDM System and initiate the role request procedure. When the user reselects the desired role, the RIDP process will be aware of the previous failed attempt and the Role Request UI displays a message which asks if Experian has been contacted.
2. Click the “I have already verified my identity with Experian” check box if Experian has been contacted.
3. Click the Next button.

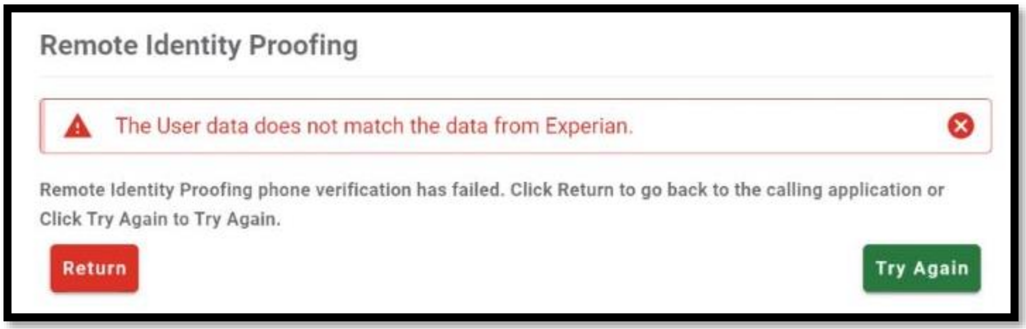
[116] Phone Proofing only occurs if the user fails the online RIDP process.

[117] Users who reside at foreign addresses will not be able to perform Phone Proofing, because it is only available for users who reside at US addresses.

4. The Identity Information Verification form is displayed. [118, 119]
5. Verify that the identity information which was proofed on the phone matches the data in the form.
6. Click the Next button.
7. Click the OK button. The user is returned to the Role Request UI to complete the role request procedure. [120]

13.5.1 RIDP Phone Verification Failure

The Role Request UI displays the error message illustrated in Figure 76: RIDP Phone Verification Failure if the identity information fails to match Experian's data after having spoken with Experian on the telephone.



Remote Identity Proofing

The User data does not match the data from Experian.

Remote Identity Proofing phone verification has failed. Click Return to go back to the calling application or Click Try Again to Try Again.

Figure 76: RIDP Phone Verification Failure

1. Click the Try Again button.
2. The Identity Information Verification form displays. [121, 122]
3. Verify that the identity information which was proofed on the phone matches the data in the form.
4. Click the Next button. [123]

13.5.2 Remote Identity Proofing (RIDP) for HDT

As described in section *13 Remote Identity Proofing*, RIDP is the process of validating sufficient information about you (e.g., credit history, personal demographic information, and other

[118] The Identity Information Verification form must contain the exact same information that was used to successfully identify the user on the phone with Experian. The IDM System compares Experian's information with the information that was entered into the form.

[119] The same spelling and syntax must be used because typographical errors (even accidental ones) will cause this step to fail.

[120] If an error occurs, proceed to section *13.5.1 RIDP Phone Verification Failure*.

[121] The Identity Information Verification form must contain the exact same information that was used to successfully identify the user on the phone with Experian. The IDM System compares Experian's information with the information that was entered into the form.

[122] The same spelling and syntax must be used because typographical errors (even accidental ones) will cause this step to fail.

[123] The Return button terminates the RIDP procedure. Termination of the RIDP process causes the role request process to fail.

indicators) to uniquely identify you. RIDP is a required service for new HETS Desktop (HDT) Users – existing HDT Users will not be required to complete the RIDP process. CMS uses Experian to remotely perform identity proofing.

The RIDP process for HDT is outlined in section *12.1 How to Request Access and Role to the HDT Application*, steps 1-4. If Experian cannot identity proof you online, you will be asked to contact either the Experian Help Desk or the MCARE Help Desk, depending on the reason you failed RIDP.

The CMS IDM System will provide you with a reference number to track your case if you cannot complete identity proofing. The Experian Help Desk cannot assist you if you do not have the reference number. The Experian Help Desk can be contacted at 1-866-578-5409. The Experian Help Desk is open Monday through Friday from 8:30 AM to 10:00 PM, Saturday from 10:00 AM to 8:00 PM, and Sunday from 11:00 AM to 8:00 PM, Eastern Standard Time.

For additional information, please see the Experian Consumer Assistance site: Experian Customer Assistance.

If you are asked to contact the MCARE Help Desk, you will be given a response code to help the MCARE Help Desk perform the manual identity proofing process with you. Please contact MCARE via the information provided in section *17.3 Support Information* of this guide.

14. Using the HDT Application

The following sub-sections provide detailed, step-by-step instructions on how to use the various features of the HDT application.

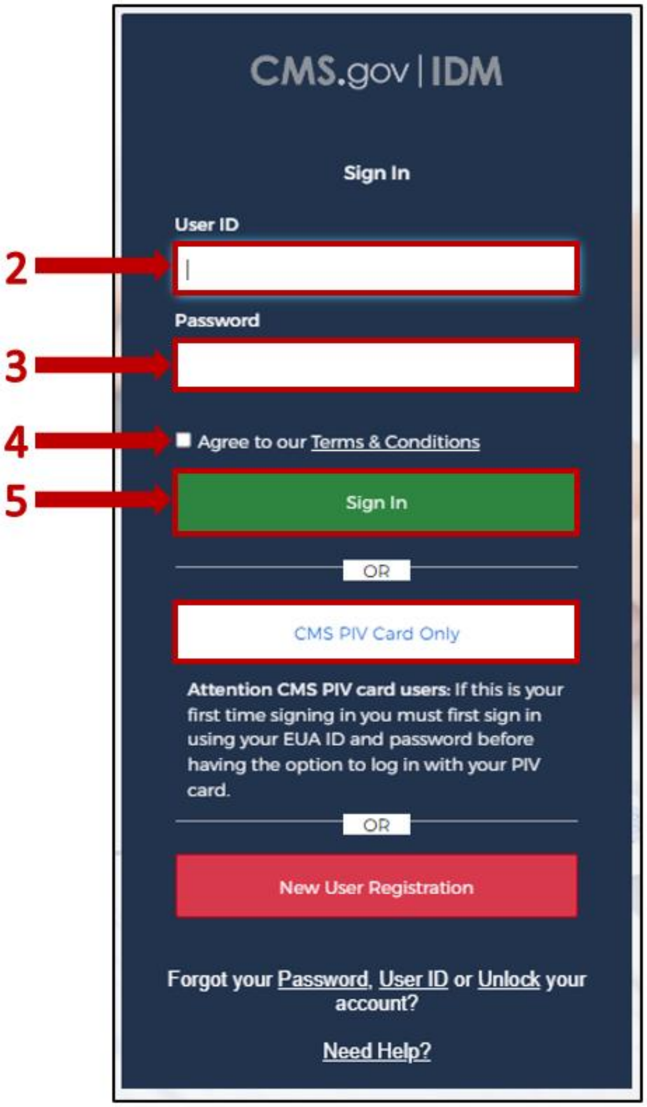
14.1 Log In to the HDT Application

HDT uses the IDM System to authenticate each user and permits that user to access the application. This section provides the steps that users must follow to sign in to HDT via the CMS IDM System.

1. Enter the CMS Applications Portal URL in a web browser:

   https://HDT.hetsp-haa.cms.gov/HDT/

   Please do not bookmark this or any other page in your internet browser. CMS discourages Users from utilizing browser bookmarks with the HDT application. The CMS IDM System Screen displays as illustrated in Figure 77: IDM System Sign-In Window.

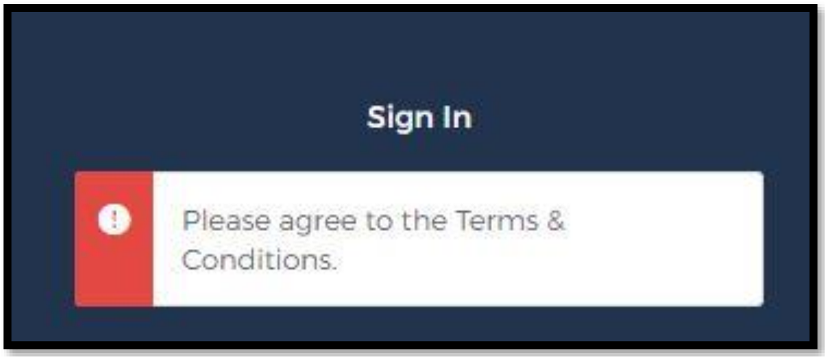


Attention CMS PIV card users: If this is your first time signing in you must first sign in using your EUA ID and password before having the option to log in with your PIV card.

Forgot your Password, User ID or Unlock your account?

Figure 77: IDM System Sign-In Window

2. Type the User ID into the Username field.
3. Type the Password into the Password field.
4. Click the check box to acknowledge agreement with the Terms & Conditions. Failure to click the check box will result in an error as illustrated in Figure 78: An Example Sign in Error: Agree to Terms & Conditions.



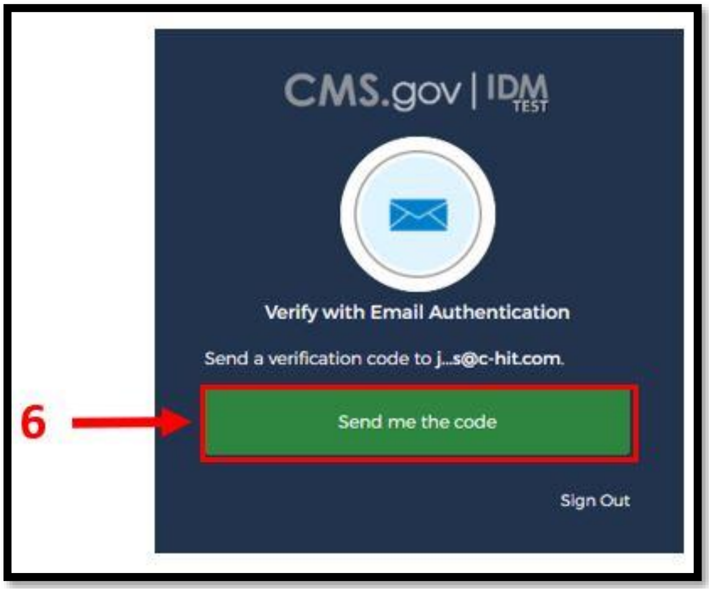
Sign In

Please agree to the Terms & Conditions.

Figure 78: An Example Sign in Error: Agree to Terms & Conditions

5. Click the Sign In button. The MFA One-time Password (OTP) Request window appears.

Note: The IDM System uses Email MFA by default, so the steps provided in this procedure follow that default. Users with alternative MFA devices should use the appropriate procedure for that MFA device.

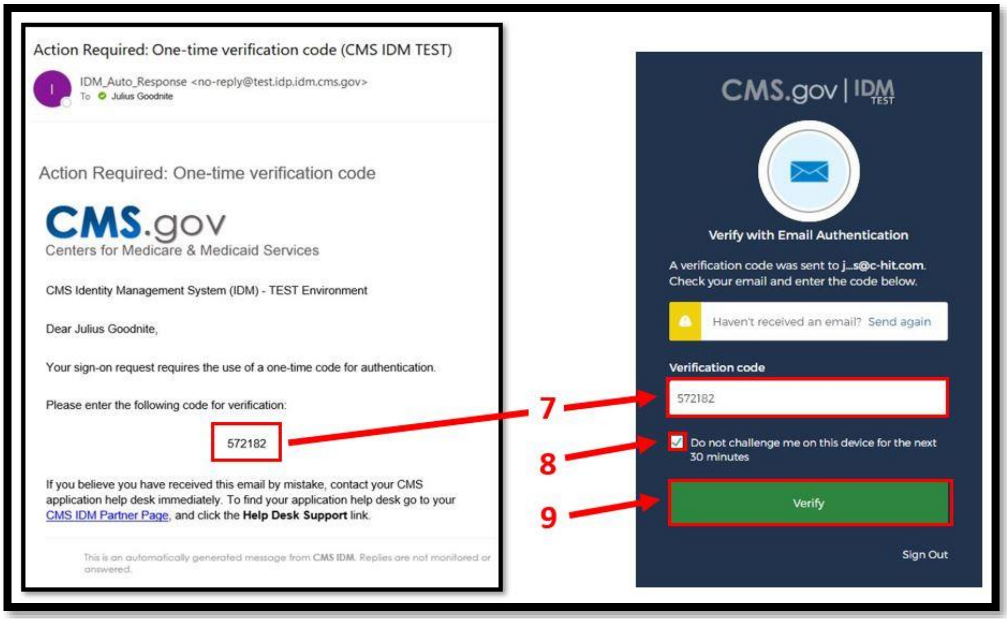


Send a verification code to j...s@c-hit.com.

Figure 79: MFA OTP Request Window

6. Click the Send me the code button to request an OTP when the Verify with Email Authentication window appears.

   The IDM System also allows the use of other MFA devices. The OTP delivery method could be an email, a voice message, a text message, or a push notification based on the user’s MFA device choice.



Action Required: One-time verification code (CMS IDM TEST)

IDM_Auto_Response <no-reply@test.idp.idm.cms.gov>
To Julius Goodnite

Action Required: One-time verification code

CMS.gov
Centers for Medicare & Medicaid Services

CMS Identity Management System (IDM) - TEST Environment

Dear Julius Goodnite,

Your sign-on request requires the use of a one-time code for authentication.

Please enter the following code for verification:

572182

If you believe you have received this email by mistake, contact your CMS application help desk immediately. To find your application help desk go to your CMS IDM Partner Page, and click the **Help Desk Support** link.

This is an automatically generated message from CMS IDM. Replies are not monitored or answered.

CMS.gov | IDM TEST

Verify with Email Authentication

A verification code was sent to **j...s@c-hit.com**. Check your email and enter the code below.

Haven't received an email? Send again

Verification code: 572182

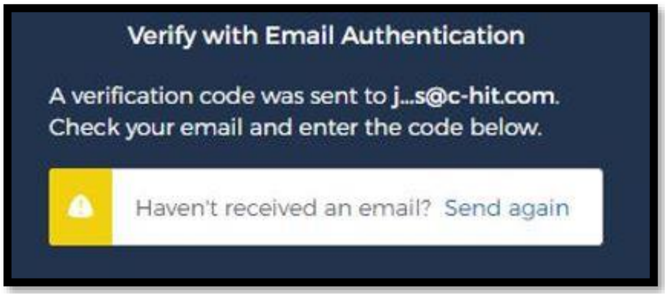
☑ Do not challenge me on this device for the next 30 minutes

Figure 80: Sample MFA OTP Email and the MFA Verification Window

7. The MFA device returns an OTP. Type the OTP into the Verification Code field. If the MFA device uses push notifications, a code is not required.

Note(s):

- The user must enter the OTP within approximately 30 seconds of completing Step 6 or the Sign-In window displays a message that asks, “Haven’t received an email? Send again.” as illustrated by Figure 81: MFA OTP Notification with Send Again Request Link.
- The user may click the Send again link to request another OTP if the original OTP request failed.



Verify with Email Authentication

A verification code was sent to **j...s@c-hit.com**. Check your email and enter the code below.

Haven't received an email? Send again

Figure 81: MFA OTP Notification with Send Again Request Link

8. (Optional) Click the checkbox to select the option “Do not challenge me on this device for the next 30 minutes”.

If this step is performed, users bypass the MFA verification phase of the authentication process if they sign out and sign back in to the system within 30 minutes of completing this MFA verification event.

9. Click the Verify button.
    - **Successful Sign-In**: The user is taken to the HETS Desktop Home Screen (HDT-1000) as illustrated by Figure 82: HETS Desktop Home Screen (HDT-1000).
    - **Unsuccessful Sign-In**: Take corrective action based on the error message that displays. Additionally, verify the accuracy of the user ID and password and attempt to sign in again.

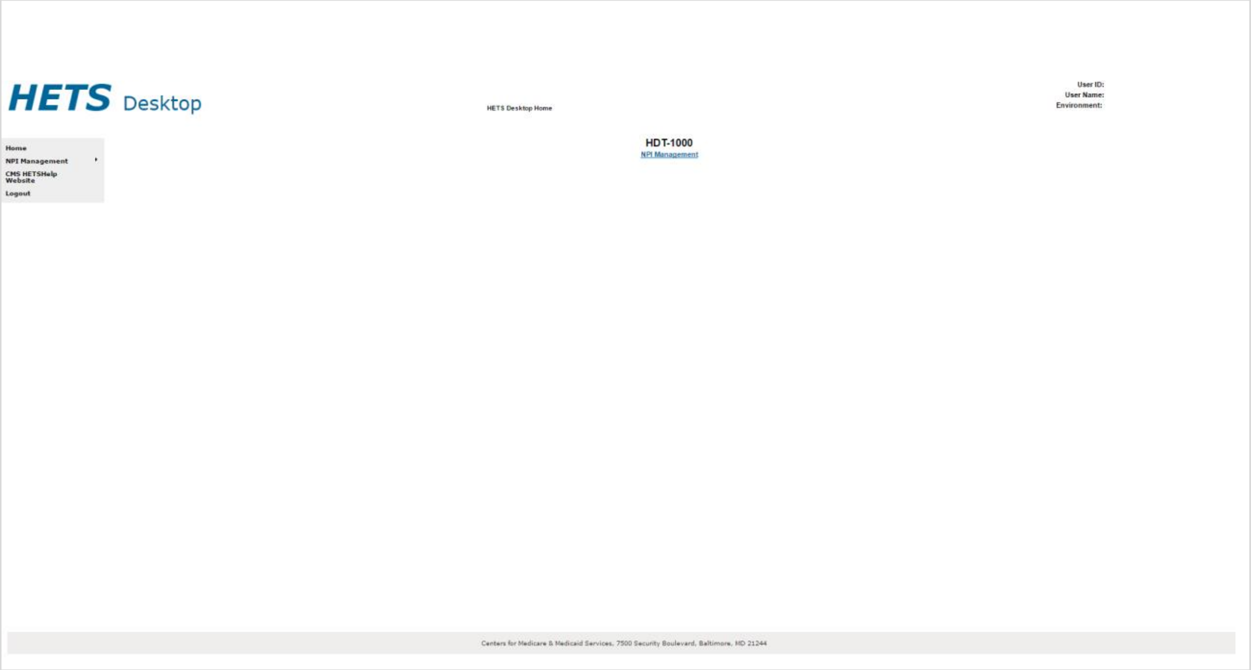


Figure 82: HETS Desktop Home Screen (HDT-1000)

When users log in to the HDT application, the HETS Desktop Home Screen (HDT-1000) displays as illustrated in Figure 82: HETS Desktop Home Screen (HDT-1000).

Users can access the functionality of the HDT application by selecting the hyperlinks from the left navigation bar. Users may also select the hyperlinks in the dynamic content area in the middle of the screen.

The navigation hyperlinks are:

- **Home** – The HDT User Interface home page.
- **NPI Management** – Allows Submitters to add, terminate and/or query NPI numbers one at a time. This link is available to Clearinghouse and Direct Provider Submitters.
- **NPI Batch Management** – Provides a link to the Enterprise File Transfer (EFT) system. This link is available only to Clearinghouse Submitters.
- **CMS HETSHelp Website** – Provides links to the CMS HETSHelp Website.

- **Logout –** Closes the active HDT application session and redirects the User to the CMS IDM System Web Access Management (Logout) Screen as illustrated in *Figure 84: CMS IDM System Web Access Management (Logout) Screen*.

14.2 Application Layout

The application layout in the Site Map, as illustrated in Figure 83: HDT Application Site Map, is outlined as follows:

The links to navigate through the HDT application are:

- Home
- NPI Management
    - NPI Management (data entry screen)
    - NPI Batch Management (available for Clearinghouse Submitters only)
- Logout

The links external to the HDT application are:

- CMS HETSHelp Website

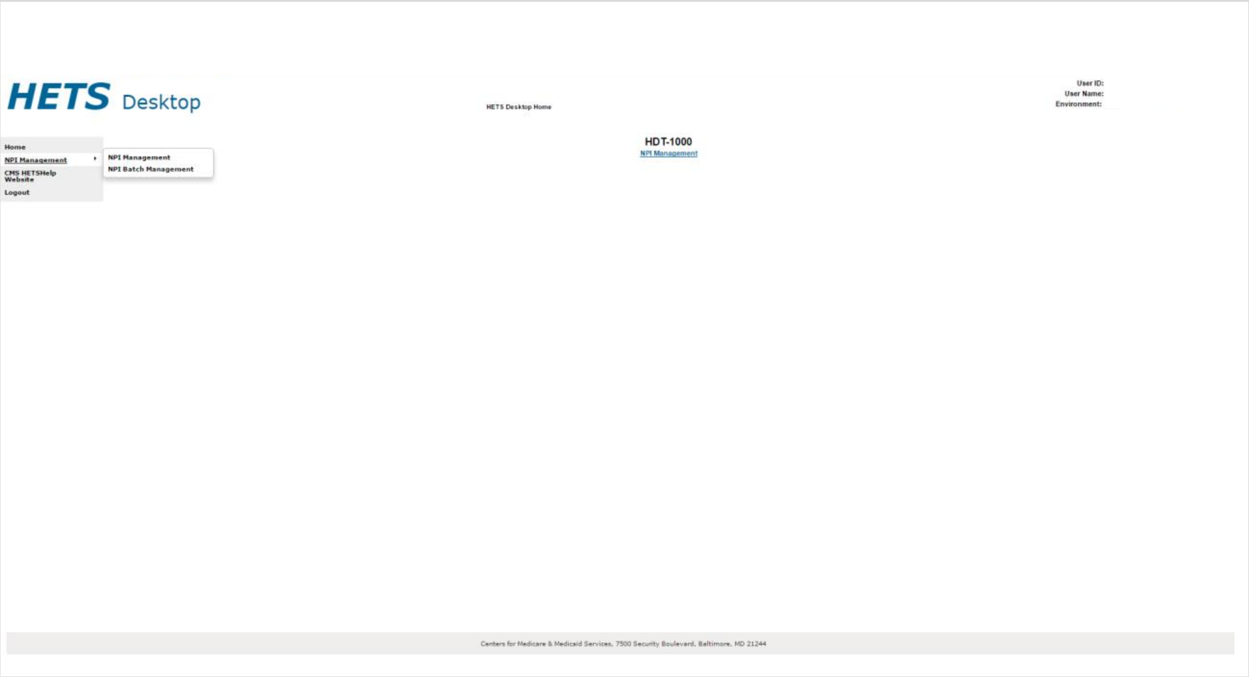
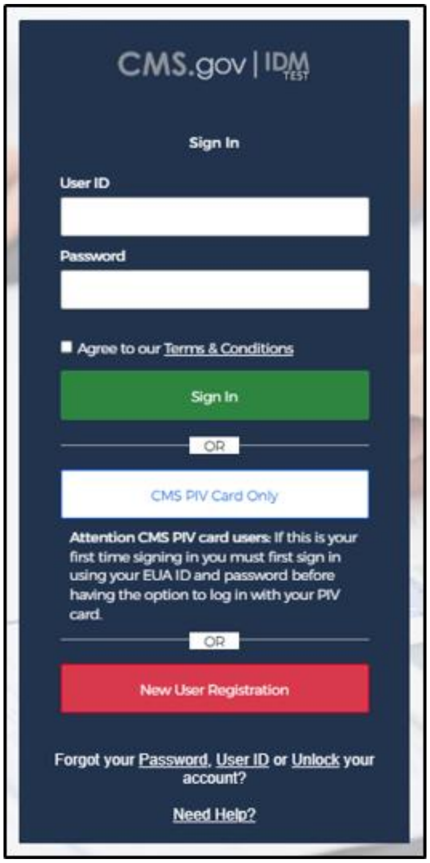


Figure 83: HDT Application Site Map

14.3 Exiting the Application

Select the [Logout] link in the left navigation menu of any screen in the HDT Application to log out from the HDT application. You will be logged out of the HDT application and redirected to the CMS IDM (Logout) Screen as illustrated by Figure 84: CMS IDM System Web Access Management (Logout) Screen.



Attention CMS PIV card users: If this is your first time signing in you must first sign in using your EUA ID and password before having the option to log in with your PIV card.

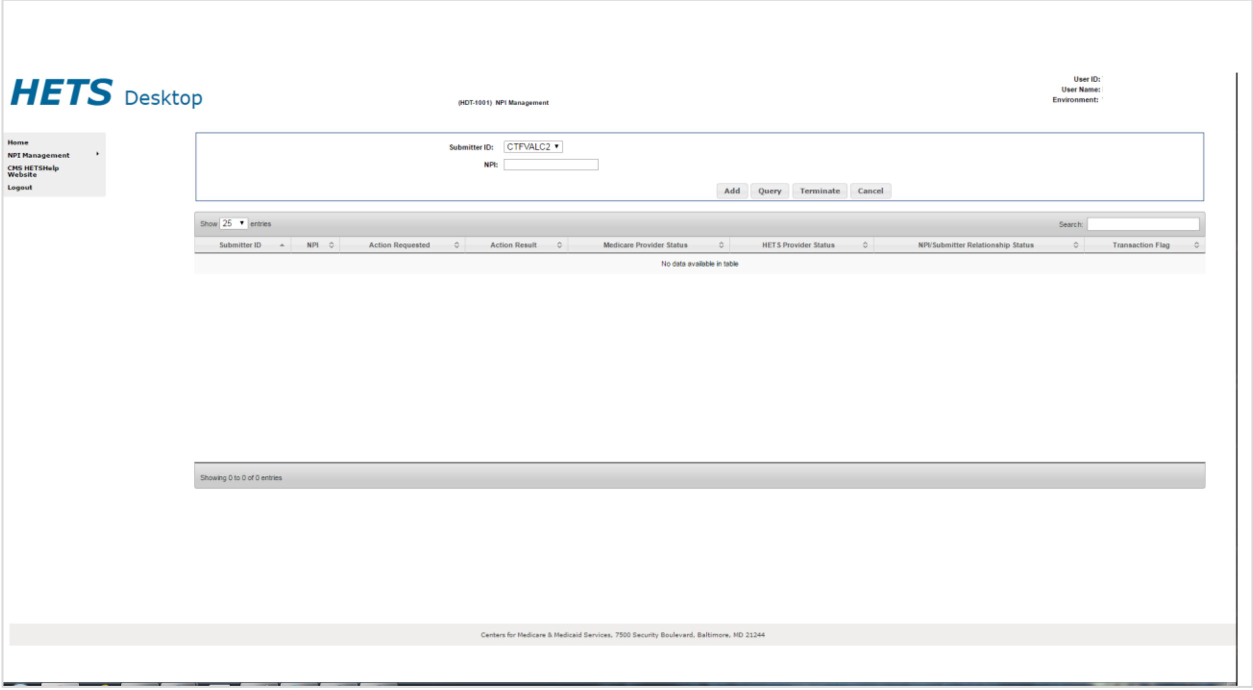
Forgot your Password, User ID or Unlock your account?

Figure 84: CMS IDM System Web Access Management (Logout) Screen

15. NPI Management (HDT-1001)

NPI Management allows Clearinghouse and Direct Provider Submitters to query, add, or terminate NPI numbers one at a time.

To access the NPI Management feature, select the [NPI Management] link in the left-hand navigation menu. The HDT NPI Management Screen (HDT-1001) displays as illustrated in Figure 85: HDT NPI Management Screen (HDT-1001).



Submitter ID: CTFVALC2

NPI:

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
No data available in table							

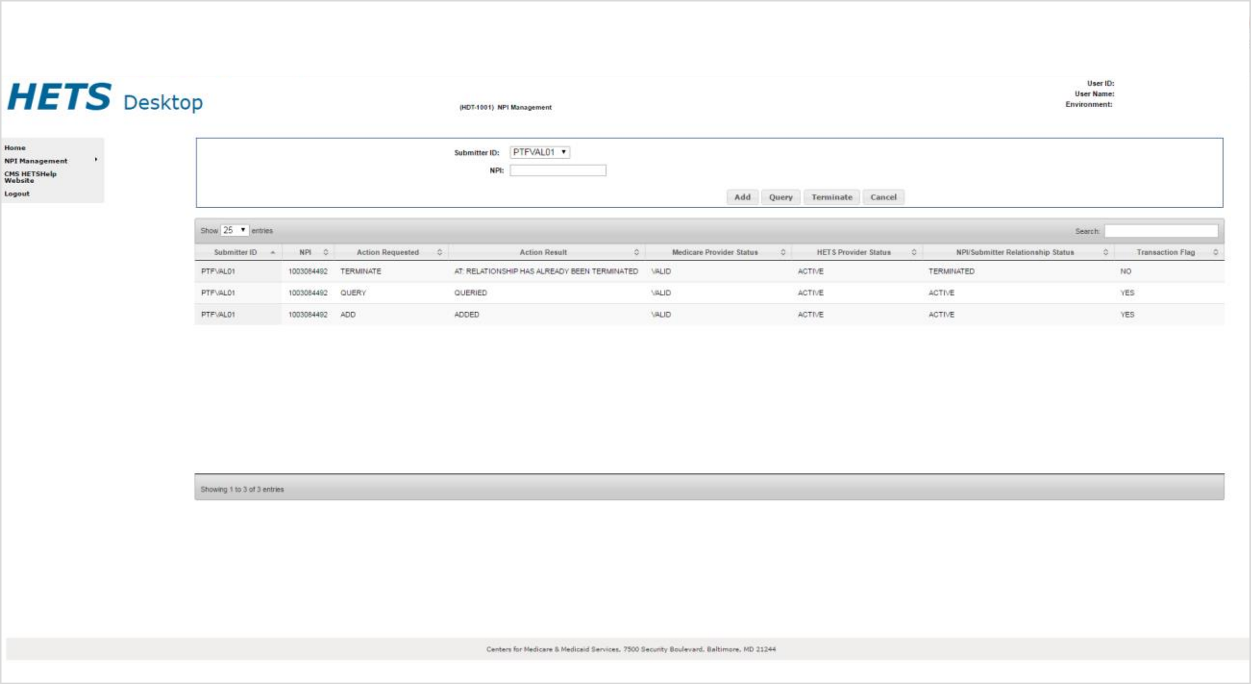
Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 85: HDT NPI Management Screen (HDT-1001)

1. Select the appropriate HETS 270/271 Submitter ID from the drop-down menu (depending on the related organization, there may only be one value present).
2. Enter an NPI value in the NPI field (HDT only accepts numeric values in this field).
3. Select [Add], [Query], [Terminate] or [Cancel] to proceed with the requested action.

Results for requested actions are displayed in an NPI Results table as illustrated in Figure 86: HDT NPI Management Screen (HDT-1001) – Results.



Submitter ID: PTFVAL01
NPI:

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
PTFVAL01	1003084492	TERMINATE	AT: RELATIONSHIP HAS ALREADY BEEN TERMINATED	VALID	ACTIVE	TERMINATED	NO
PTFVAL01	1003084492	QUERY	QUERIED	VALID	ACTIVE	ACTIVE	YES
PTFVAL01	1003084492	ADD	ADDED	VALID	ACTIVE	ACTIVE	YES

Showing 1 to 3 of 3 entries

Figure 86: HDT NPI Management Screen (HDT-1001) – Results

The following information is provided for each action selected:

- Submitter ID – the 8-character Submitter ID selected by the User.
- NPI – NPI entered by the User.
- Action Requested – the action button selected by the User. Values include:
  - Query – the User selects this action to determine the status of the relationship between the Submitter ID and the NPI entered.
  - Add – the User selects this action to create a relationship between a Submitter ID and an NPI for the purpose of submitting 270 request transactions via the HETS 270/271 application.
  - Terminate – this action is selected by the User when a Submitter no longer has a business relationship with an NPI.
- Action Result – the result returned by HDT based on the action selected by the User. Values include:
  - Queried – the query request has been processed by the HDT application and the query results are displayed in the NPI results table.
  - Added – the NPI/Submitter relationship has been added to the HDT application.
  - AE: Relationship Already Exists – the NPI/Submitter relationship already exists and cannot be added.
  - SP: Relationship is Suspended – the NPI/Submitter relationship is currently suspended and cannot be added.
  - IM: Invalid Medicare Provider Status – the Medicare Provider Status is invalid and cannot be added.

  - Terminated – the NPI/Submitter relationship has been terminated in the HDT application.
  - AT: Already Terminated – the NPI/Submitter relationship is already terminated and cannot be terminated.
  - NE: Relationship Does Not Exist – the NPI/Submitter relationship does not exist and cannot be terminated.
  - VA: No Relationship with VA – the NPI/Submitter relationship cannot be added as the NPI belongs to a VA facility.
- Medicare Provider Status – this status indicates whether the NPI is an active, valid FFS Medicare Provider. Values include:
  - Valid – the provider is an active, valid FFS Medicare provider or supplier.
  - Invalid – the provider is not an active, valid FFS Medicare provider or supplier.
- HETS Provider Status – this is the status of the NPI for the HETS 270/271 application. Values include:
  - Active – the NPI is active for the HETS 270/271 application.
  - Suspended – the NPI is suspended for the HETS 270/271 application.
  - Terminated – the NPI is terminated for the HETS 270/271 application.
  - Not Found – the NPI is not on file for the HETS 270/271 application.
- NPI/Submitter Relationship Status – this is the status of the NPI/Submitter relationship for the HETS 270/271 application. Values include:
  - Active – the NPI/Submitter Relationship is active for the HETS 270/271 application.
  - Suspended – the NPI/Submitter Relationship is suspended for the HETS 270/271 application.
  - Terminated – the NPI/Submitter Relationship is terminated for the HETS 270/271 application.
  - Not Found – the NPI/Submitter Relationship is not on file for the HETS 270/271 application.
  - Expired – the NPI/Submitter Relationship is expired for the HETS 270/271 application.
- Transaction Flag – this status flag indicates whether transactions with the HETS 270/271 application are permitted. Values include:
  - Yes – Indicates that transactions with the HETS 270/271 application are permitted. This value is returned when all conditions are met:
    - Submitter Status = “Active”, AND
    - Medicare Provider Status = “Valid”, AND
    - HETS Provider Status = “Active”, AND
    - NPI/Submitter Relationship Status = “Active”.

- No – Indicates that transactions with the HETS 270/271 application are not permitted. This value is returned when any of these conditions are met:
  - Submitter Status <> “Active”, OR
  - Medicare Provider Status <> “Valid”, OR
  - HETS Provider Status <> “Active”, OR
  - NPI/Submitter Relationship Status <> “Active”.

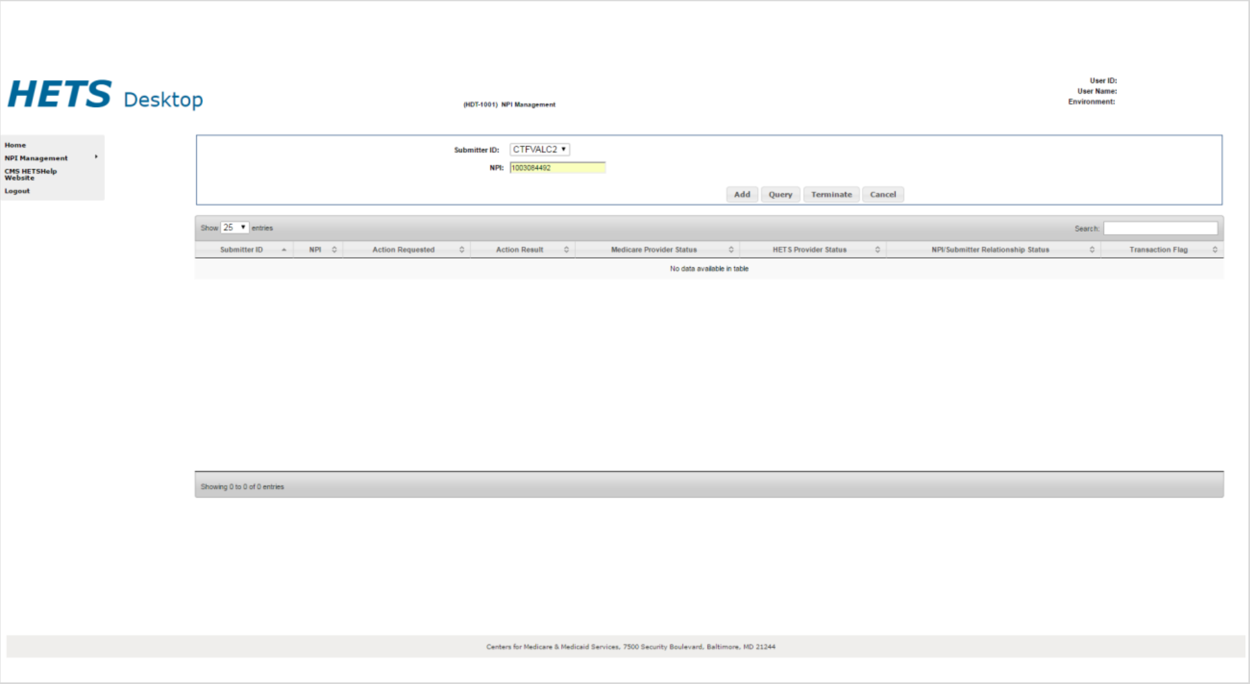
Note: The table will display the results in the order in which the NPIs are entered into the NPI text box, with the most recent action listed first. The HDT application defaults to display up to 25 rows in the NPI Results table. The user can change this value in the ‘Show Entries’ drop-down to modify the results parameters.

15.1 Query

15.1.1 Action

The Query action allows Submitters to verify NPI numbers prior to submitting a 270 request transaction to the HETS 270/271 application. Responses are returned to the screen in a matter of seconds.

To perform a query action, follow these steps on the HDT User Interface NPI Management Screen as illustrated in Figure 87: HDT NPI Management Screen (HDT-1001) – Query.



Submitter ID: CTFVALC2

NPI: 1003084492

Show 25 entries

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
No data available in table							

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 87: HDT NPI Management Screen (HDT-1001) – Query

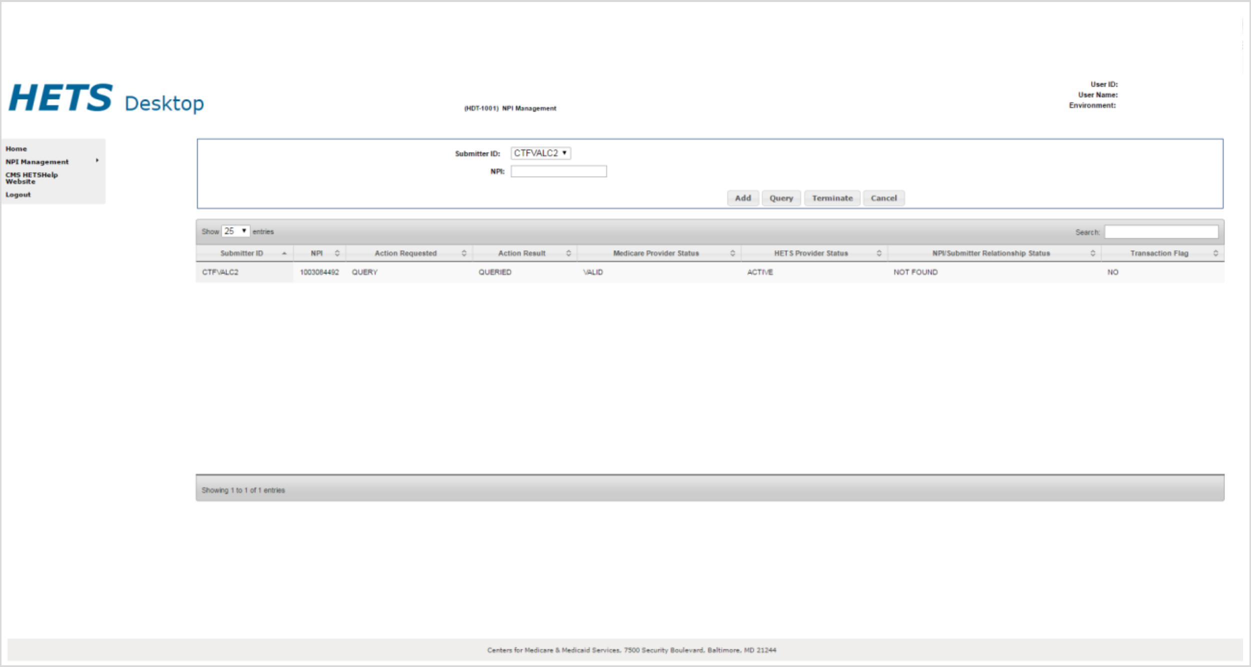
1. Select a Submitter ID from the drop-down list labeled Submitter ID.

2. Enter a 10-digit NPI number in the NPI field. HDT only accepts numeric values in the NPI field.
3. Select [Query].

> **Note:** The HDT application will clear the NPI field when users select an NPI Management action. The Submitter ID field will not be cleared. If users wish to perform actions for a different Submitter ID associated with their Submitter Profile, they must select that Submitter ID from the Submitter ID drop-down list.

15.1.2 Result

Figure 88: HDT NPI Management Screen (HDT-1001) – Query Results displays the NPI Results table for the query action.



Submitter ID: CTFVALC2

NPI:

Show 25 entries

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
CTFVALC2	1003084492	QUERY	QUERIED	VALID	ACTIVE	NOT FOUND	NO

Showing 1 to 1 of 1 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

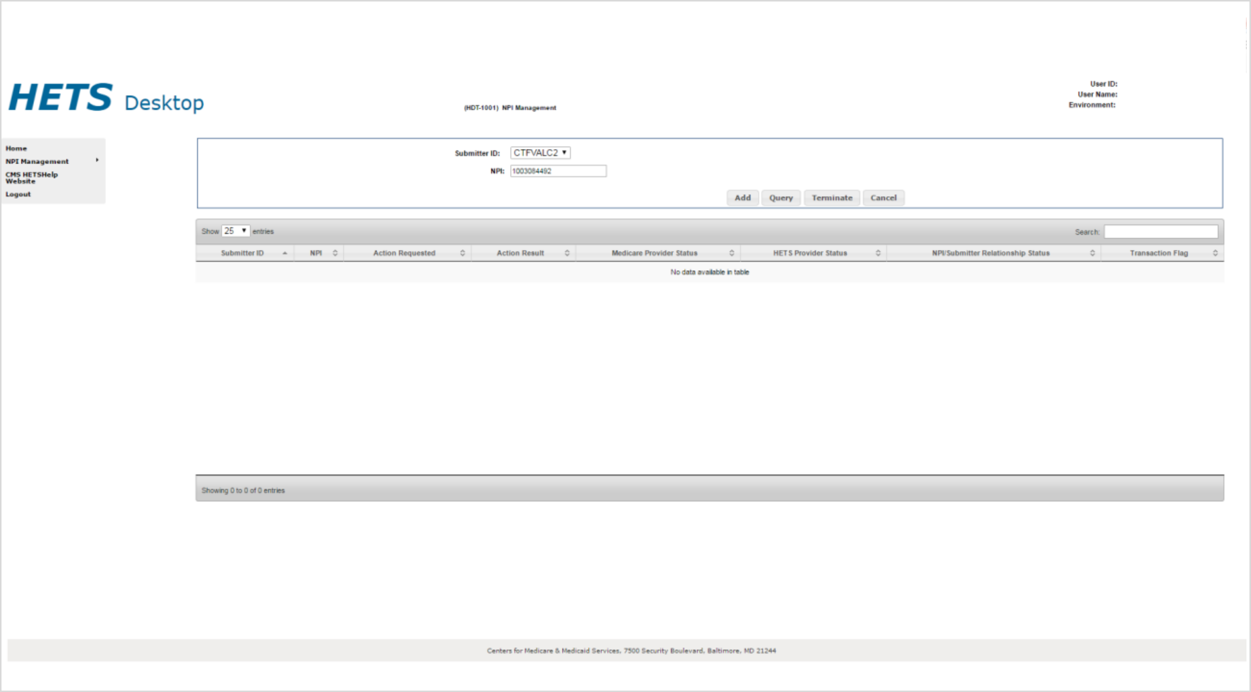
Figure 88: HDT NPI Management Screen (HDT-1001) – Query Results

15.2 Add

The Add action creates a relationship between a Submitter ID and an NPI necessary for 270 request transactions to successfully process via the HETS 270/271 application. If users send an eligibility request with an NPI number that is not on file with CMS, is not a valid FFS Medicare Provider at the time the request is processed, or is not associated with the Submitter, then a 271 AAA error will be returned instead of entitlement information.

15.2.1 Action

To perform the Add action, follow these steps on the HDT User Interface NPI Management Screen as illustrated in Figure 89: HDT NPI Management Screen (HDT-1001) – Add.



(HDT-1001) NPI Management

Submitter ID: CTFVALC2

NPI: 1003084492

Show 25 entries

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
No data available in table							

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

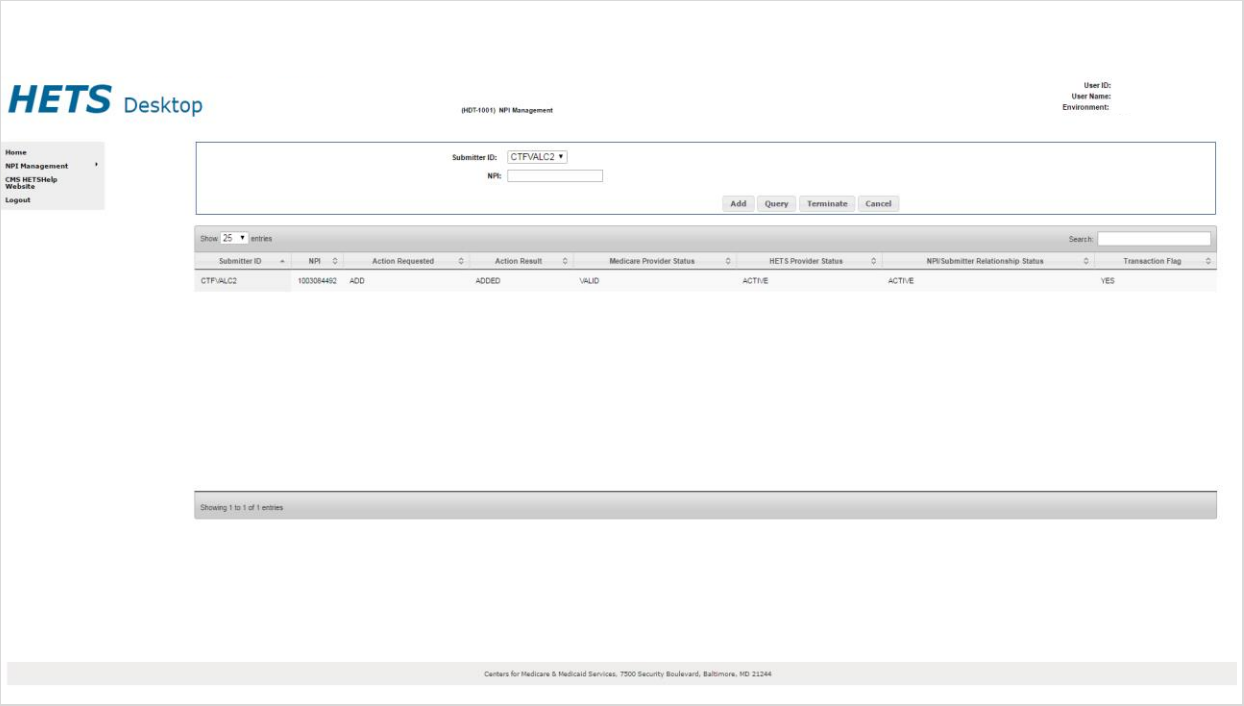
Figure 89: HDT NPI Management Screen (HDT-1001) – Add

1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the NPI field. HDT only accepts numeric values in the NPI field.
3. Select [Add].

Note: The HDT application will clear the NPI field when users select an NPI Management action. The Submitter ID field will not be cleared. If users wish to perform actions for a different Submitter ID associated with their Submitter Profile, they must select that Submitter ID from the Submitter ID drop-down list.

15.2.2 Result

Figure 90: HDT NPI Management Screen (HDT-1001) – Add Results displays the NPI Results table for the Add action.



Submitter ID: CTFVALC2

NPI:

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
CTFVALC2	1003084492	ADD	ADDED	VALID	ACTIVE	ACTIVE	YES

Showing 1 to 1 of 1 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

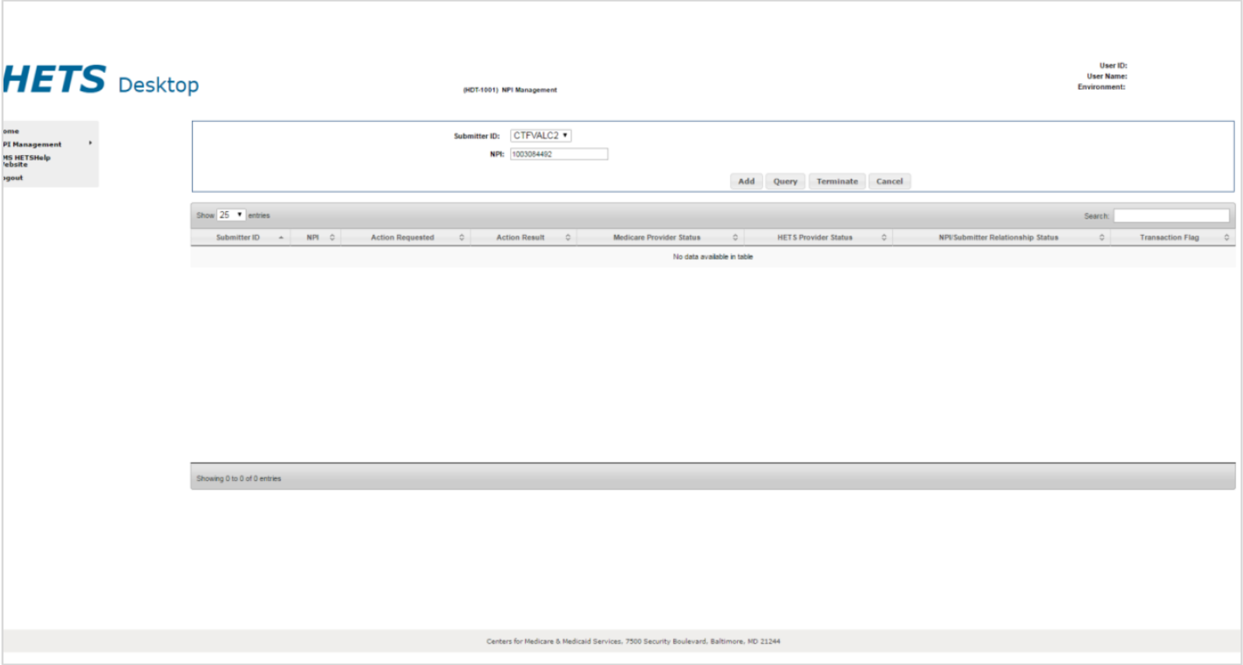
Figure 90: HDT NPI Management Screen (HDT-1001) – Add Results

15.3 Terminate

The terminate action ends a relationship between a Submitter ID and an NPI when there is no longer a business relationship between them. Once a relationship is terminated, users will be unable to submit eligibility transactions via the HETS 270/271 application for the NPI.

15.3.1 Action

To perform the terminate action, follow these steps on the HDT NPI Management – Terminate Screen as illustrated in Figure 91: HDT User Interface NPI Management Screen (HDT-1001) – Terminate.



Submitter ID: CTFVALC2

NPI: 1003064492

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
No data available in table							

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

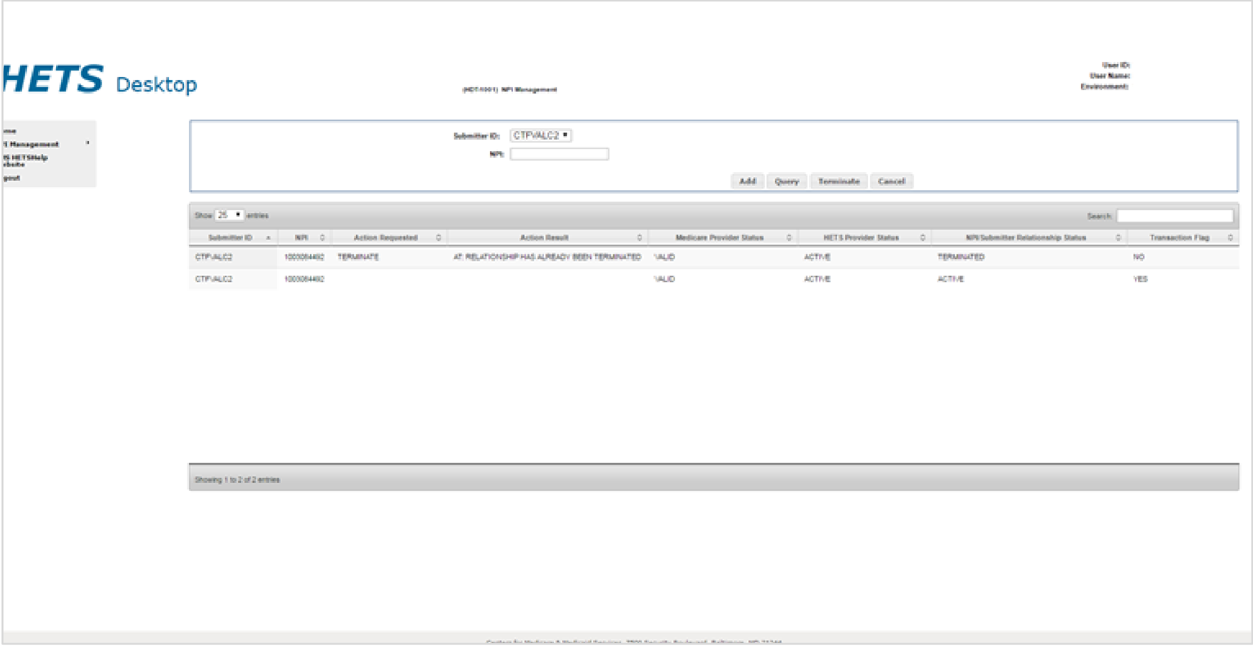
Figure 91: HDT User Interface NPI Management Screen (HDT-1001) – Terminate

1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the NPI field. HDT only accepts numeric values in the NPI field.
3. Select [Terminate].

Note: The HDT application will clear the NPI field when users select an NPI Management action. The Submitter ID field will not be cleared. If users wish to perform actions for a different Submitter ID associated with their Submitter Profile, they must select that Submitter ID from the Submitter ID drop-down list.

15.3.2 Result

Figure 92: HDT NPI Management Screen (HDT-1001) – Terminate Results displays the NPI Results table for the terminate action.



Submitter ID: CTPVALC2

NPI:

Show 25 entries

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
CTPVALC2	1003084492	TERMINATE	AT: RELATIONSHIP HAS ALREADY BEEN TERMINATED	VALID	ACTIVE	TERMINATED	NO
CTPVALC2	1003084492			VALID	ACTIVE	ACTIVE	YES

Showing 1 to 2 of 2 entries

Figure 92: HDT NPI Management Screen (HDT-1001) – Terminate Results

16. NPI Batch Management

NPI Batch Management is available to Clearinghouse Submitters only. This feature allows users to query, add, and/or terminate more than one NPI number at a time.

The NPI Batch Management screen allows users to complete the following:

- File Upload
- File Download
- View uploaded files
- View processed files
- Cancel actions

Note: Clearinghouse Submitters are limited to uploading only one batch file per day. If a Clearinghouse Submitter attempts to upload more than one file during a single calendar day, an error message is returned in the batch output file.

To access the NPI Management feature, select the [NPI Batch Management] link in the left navigation menu as illustrated in Figure 93: NPI Batch Management Menu Navigation below. The HDT NPI Batch Management Screen (HDT-1002) displays as described in 16.3.

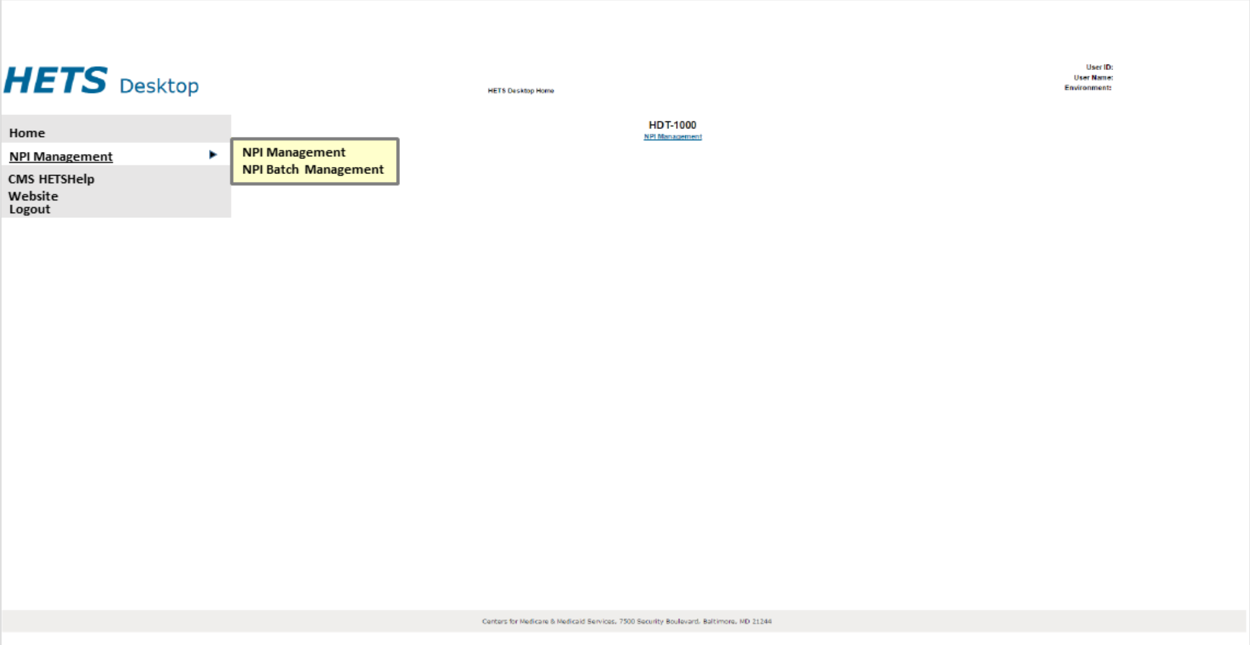


Figure 93: NPI Batch Management Menu Navigation

16.1 Input File

The required naming convention for the batch input file is:

SubmitterID.IN.HDT.EFT

Customizable elements:

SubmitterID = The HETS Submitter ID assigned to your organization by CMS. (Example: C123A456).

All other file name elements are required and constant.

Sample input file name: File Name: C123A456.IN.HDT.EFT

The acceptable file format for the NPI Batch Management input file is a comma delimited, flat text file. The input file consists of three data elements per line – Submitter ID, NPI and Action. Refer to for the Input File Layout and a description of elements.

Table 11: Input File Layout and Element Description

Data Element	Data Type	Length	Possible Values	Description
Submitter ID	Alphanumeric	8	N/A	The 8-character Submitter ID associated with the Clearinghouse.
NPI	Numeric	10	N/A	The 10-digit NPI for whom the Clearinghouse sends eligibility transactions to the HETS 270/271 application.
Action	Alpha	1	Q, A, or T	The action requested by the Clearinghouse to query the current status of, to add, or to terminate a relationship with an NPI. Values include: Q: Request a query of the relationship between the Submitter ID and the NPI. A: Request to add a relationship between the Submitter ID and the NPI. T: Request to terminate the relationship between the Submitter ID and the NPI.

Sample Input File

File Name: C123A456.IN.HDT.EFT

```
C123A456,1111111111,Q
C123A456,2222222222,Q
C123A456,3333333333,A
C123A456,3333333333,A
C123A456,4444444444,A
C123A456,5555555555,A
C123A456,6666666666,T
C123A456,6666666666,T
C123A456,7777777777,T
```

16.2 Output File

The system generated naming convention for the batch output file is:

SubmitterID.OUT.HDT.EFT.D{date}.T{time}

System defined elements:

SubmitterID = The HETS Submitter ID assigned to your organization by CMS.

Dyymmdd = {Date} in yymmdd format

Thhmmsst – {Time} in hhmmsst format

All other file name elements are required and constant.

Sample output file name: File Name: C123A456.OUT.HDT.EFT.D200401.T0122331

The output file generated by the HDT application will be in the same format as the input file with exception of the addition of the date and time stamp of when the file was processed, and status responses appended to each line.

If the NPI Batch Management input file contains an NPI which is not equal to 10 characters or is not numeric, the output file will include a row for the NPI with a Medicare Provider Status of Invalid. All rows within an input file will be processed if there are no batch file errors.

Refer to Table 12: Output File Layout and a description of elements.

Table 12: Output File Layout

Data Element	Data Type	Possible Values	Description
Submitter ID	Alphanumeric	N/N/AA	The 8-character Submitter ID associated with the Clearinghouse.
NPI	Numeric	N/A	The NPI that the Clearinghouse provided on the input file.
Action Requested	Alpha	Q, A or T	The action requested by the Submitter on the input file for the NPI. Values include: Q: Request a query of the relationship between the Submitter ID and the NPI. A: Request to add a relationship between the Submitter ID and the NPI. T: Request to terminate the relationship between the Submitter ID and the NPI.

Data Element	Data Type	Possible Values	Description
Action Result	Alpha	Q, A, AE, SP, IM, T, AT, NE, or VA	The result of the action requested by the Submitter on the input file for the NPI. Values include: Q: The query request has been processed and the query results are displayed. A: The NPI/Submitter relationship has been added to the HDT application. AE: The NPI/Submitter relationship already exists and cannot be added. SP: The NPI/Submitter relationship is currently suspended and cannot be added. IM: The Medicare Provider Status is invalid and cannot be added. T: The NPI/Submitter relationship has been terminated in the HDT application. AT: The NPI/Submitter relationship is already terminated and cannot be terminated. NE: The NPI/Submitter relationship does not exist and cannot be terminated. VA: No Relationship with VA – the NPI/Submitter relationship cannot be added as the NPI belongs to a VA facility.
Submitter Status	Alpha	A, S or T	The status of the Submitter in the HDT application. Values include: A: The Submitter is active and authorized to conduct HETS 270/271 transactions. S: The Submitter is suspended and not authorized to conduct HETS 270/271 transactions. Please contact MCARE for additional information. T: The Submitter has been terminated and is not authorized to conduct HETS 270/271 transactions. Please contact MCARE for additional information.
Medicare Provider Status	Alpha	V or I	The status that indicates whether the NPI is an active, valid FFS Medicare Provider. Values include: V: The NPI is an active, valid FFS Medicare Provider. I: The NPI is not an active, valid FFS Medicare Provider.

Data Element	Data Type	Possible Values	Description
HETS Provider Status	Alpha	A, S, T or NF	The status of the NPI for the HETS 270/271 application. Values include: A: The NPI is active for the HETS 270/271 application. S: The NPI is suspended for the HETS 270/271 application. T: The NPI is terminated for the HETS 270/271 application. NF: The NPI is not on file for the HETS 270/271 application.
NPI/Submitter Relationship Status	Alpha	A, S, T, NF, or E	The status of the NPI/Submitter relationship for the HETS 270/271 application. Values include: A: The NPI/Submitter Relationship is active for the HETS 270/271 application. S: The NPI/Submitter Relationship is suspended for the HETS 270/271 application. T: The NPI/Submitter Relationship is terminated for the HETS 270/271 application. NF: The NPI/Submitter Relationship is not on file for the HETS 270/271 application. E: The NPI/Submitter Relationship is expired for the HETS 270/271 application.
Transaction Flag	Alpha	Y or N	The status flag that indicates whether transactions with the HETS 270/271 application are permitted. Values include: Y: Yes, transactions with the HETS 270/271 application are permitted. This value is returned when the following conditions are met: Submitter Status = A; and Medicare Provider Status = V; and HETS Provider Status = A; and NPI/Submitter Relationship Status = A N: No, transactions with the HETS 270/271 application are not permitted.

Sample Output File

File Name: C123A456.OUT.HDT.EFT,D200401.T0122331

File processed on 04/01/2020 01:22 AM

```
C123A456,1111111111,Q,Q,A,V,A,A,Y

C123A456,2222222222,Q,Q,A,I,T,T,N

C123A456,3333333333,A,A,A,V,A,A,Y

C123A456,3333333333,A,AE,A,V,A,A,Y

C123A456,4444444444,A,SP,A,V,S,S,N

C123A456,5555555555,A,IM,A,I,NF,NF,N
```

C123A456,6666666666,T,T,A,V,A,T,N

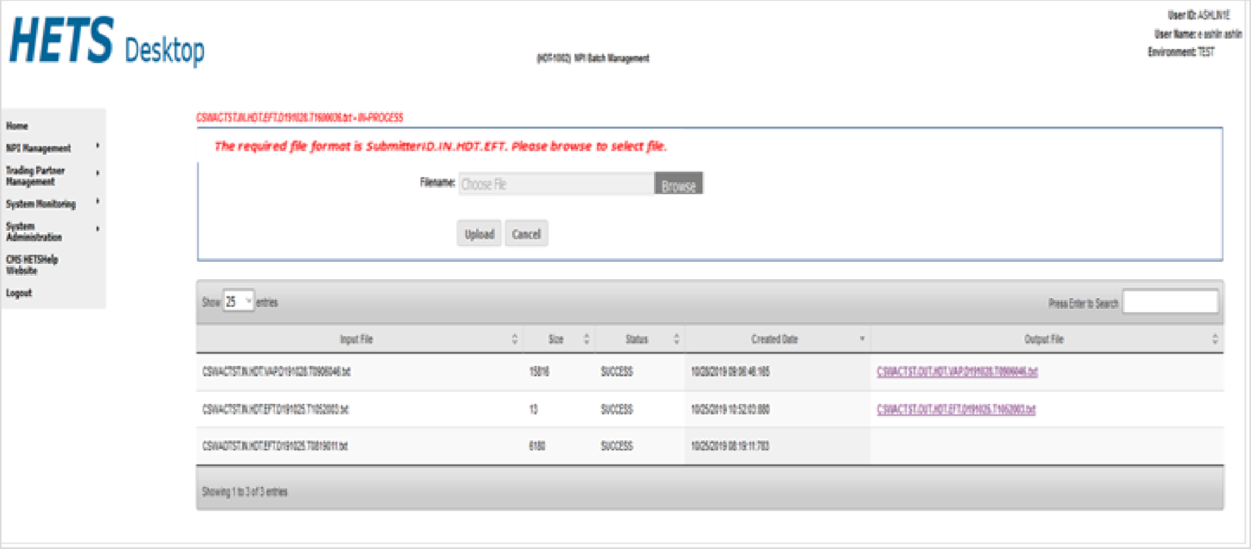
C123A456,6666666666,T,AT,A,V,A,T,N

C123A456,7777777777,T,NE,A,I,NF,NF,N

Note: The Sample Input and Output Files are for illustrative purposes only. Actual results will vary based on the status of NPIs and Submitter IDs in the HDT application.

16.3 Viewing NPI Batch Management

This is the initial landing page in the batch file section. It will display recent batch files and their results. The HDT NPI Batch Management Screen (HDT-1002) will display as illustrated in Figure 94: HDT-1002 NPI Batch Management Screen.



CSWACTST.IN.HDT.EFT.D191028.T1600036.txt - IN-PROCESS

The required file format is SubmitterID.IN.HDT.EFT. Please browse to select file.

Input File	Size	Status	Created Date	Output File
CSWACTST.IN.HDT.VAP.D191028.T0906046.txt	15816	SUCCESS	10/28/2019 09:06:46.165	CSWACTST.OUT.HDT.VAP.D191028.T0906046.txt
CSWACTST.IN.HDT.EFT.D191025.T1052003.txt	13	SUCCESS	10/25/2019 10:52:03.080	CSWACTST.OUT.HDT.EFT.D191025.T1052003.txt
CSWADTST.IN.HDT.EFT.D191025.T0819011.txt	6180	SUCCESS	10/25/2019 08:19:11.703	

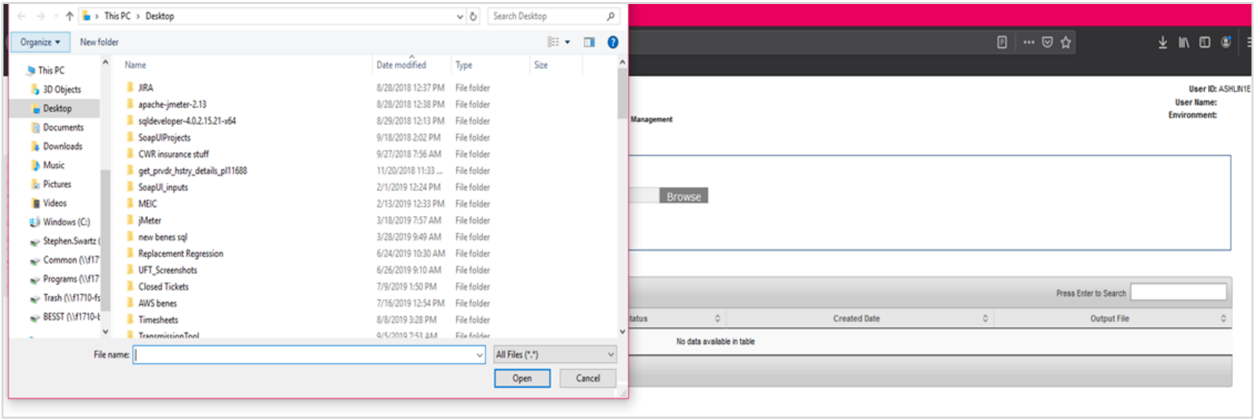
Showing 1 to 3 of 3 entries

Figure 94: HDT-1002 NPI Batch Management Screen

16.4 Uploading a File

To upload an input file, follow these steps:

1. On the HDT-1002 NPI Batch Management screen, illustrated in Figure 94: HDT-1002 NPI Batch Management Screen, select [Browse]. A pop-up will open as illustrated by Figure 95: Select Upload File for Processing and allow you to select the file from your local device.

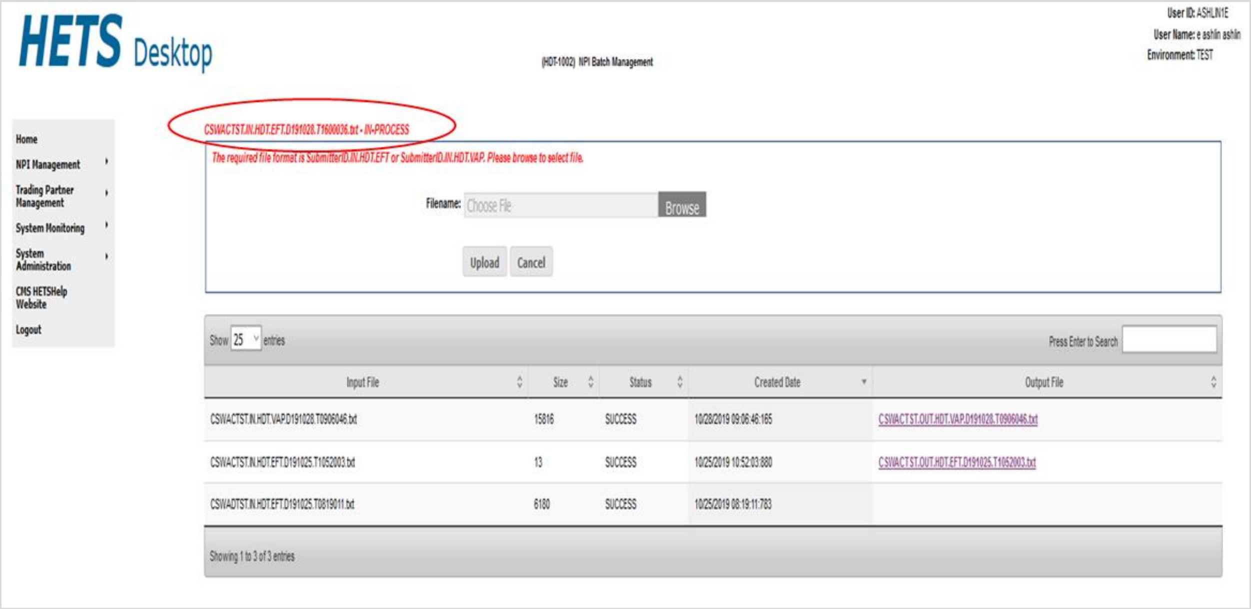


Name	Date modified	Type	Size
JIRA	8/28/2018 12:37 PM	File folder	
apache-jmeter-2.13	8/28/2018 12:38 PM	File folder	
sqldeveloper-4.0.2.15.21-x64	8/29/2018 12:13 PM	File folder	
SoapUIProjects	9/18/2018 2:02 PM	File folder	
CWR insurance stuff	9/27/2018 7:56 AM	File folder	
get_prvdr_hstry_details_pl11688	11/20/2018 11:33 ...	File folder	
SoapUI_inputs	2/1/2019 12:24 PM	File folder	
MEIC	2/13/2019 12:33 PM	File folder	
jMeter	3/18/2019 7:57 AM	File folder	
new benes sql	3/28/2019 9:49 AM	File folder	
Replacement Regression	6/24/2019 10:30 AM	File folder	
UFT_Screenshots	6/26/2019 9:10 AM	File folder	
Closed Tickets	7/9/2019 1:50 PM	File folder	
AWS benes	7/16/2019 12:54 PM	File folder	
Timesheets	8/8/2019 3:28 PM	File folder	
TransmissionTool	9/5/2019 7:53 AM	File folder	

tatus	Created Date	Output File
No data available in table		

Figure 95: Select Upload File for Processing

2. Select the comma delimited, flat text file containing the multiple NPIs you wish to query, add and/or terminate. Then select [Open].
3. Select [Upload]. Once the file has finished uploading, HDT will display the message “SubmitterIND.IN.HDT.EFT. YYMMDD.XXXXXXX.txt *IN-PROCESS”. The **HDT-1002 NPI Batch Management** screen will be updated to show the file in process as illustrated in Figure 96: Submitted File – In Progress Verification and Output File.



CSWACTST.IN.HDT.EFT.D191028.T1600036.txt - IN-PROCESS

The required file format is SubmitterID.IN.HDT.EFT or SubmitterID.IN.HDT.VAP. Please browse to select file.

Input File	Size	Status	Created Date	Output File
CSWACTST.IN.HDT.VAP.D191028.T0906046.txt	15816	SUCCESS	10/28/2019 09:06:46:165	CSWACTST.OUT.HDT.VAP.D191028.T0906046.txt
CSWACTST.IN.HDT.EFT.D191025.T1052003.txt	13	SUCCESS	10/25/2019 10:52:03:880	CSWACTST.OUT.HDT.EFT.D191025.T1052003.txt
CSWADTST.IN.HDT.EFT.D191025.T0819011.txt	6180	SUCCESS	10/25/2019 08:19:11:783	

Showing 1 to 3 of 3 entries

Figure 96: Submitted File – In Progress Verification and Output File

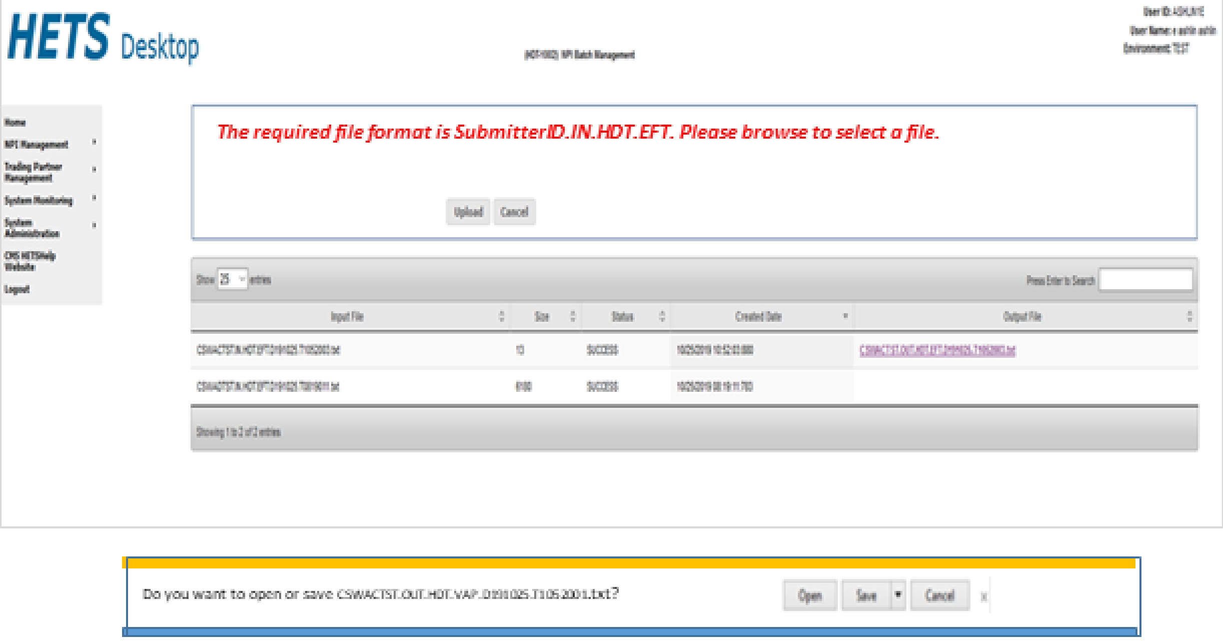
16.5 Downloading Output File

To download a results file, follow these steps:

1. Select the appropriate Output File that you would like to review. An *EFT File Download* pop-up window will display as illustrated in Figure 97: EFT File Download.
2. Select the HDT-1002 NPI Batch Management page following the steps in section *16 NPI Batch Management*. Recent batch files will display in the Submitter Output File list, including input file name, file size, file processing status, created date and, if applicable,

a link to the batch response file in the Output File column, as illustrated in Figure 97: EFT File Download.

3. Select Save. The file will be saved as the default file name of the HDT Batch output file. You may rename the file at your discretion once the file is saved to your computer.
4. Select Cancel if you decide not to save the results file.



The required file format is SubmitterID.IN.HDT.EFT. Please browse to select a file.

Input File	Size	Status	Created Date	Output File
CSWACTST.IN.HDT.EFT.D191025.T1052003.txt	13	SUCCESS	10/25/2019 10:52:03.080	CSWACTST.OUT.HDT.EFT.D191025.T1052003.txt
CSWACTST.IN.HDT.EFT.D191025.T0819011.txt	6180	SUCCESS	10/25/2019 08:19:11.783	

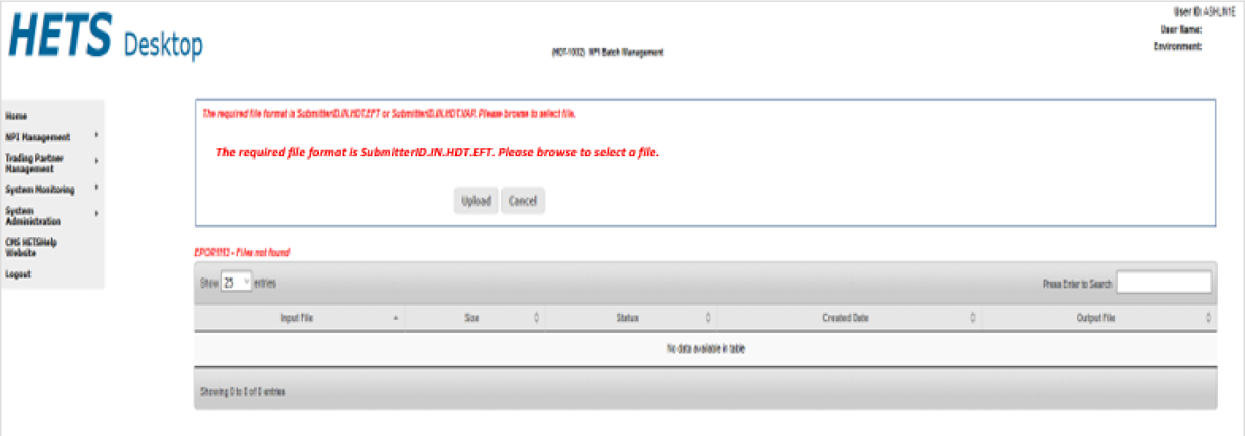
Showing 1 to 2 of 2 entries

Do you want to open or save CSWACTST.OUT.HDT.VAP.D191025.T1052001.txt?

Figure 97: EFT File Download

16.6 Invalid File Name Format Error Message

If a HDT user from a clearinghouse attempts to upload a batch input file that does not meet the required naming convention specified in section *16.1 Input File*, HDT will return an error message on the HDT-1002 NPI Batch Management page as illustrated in Figure 98: Invalid File Name Format.



The required file format is SubmitterID.IN.HDT.EFT or SubmitterID.IN.HDT.VAP. Please browse to select file.

The required file format is SubmitterID.IN.HDT.EFT. Please browse to select a file.

EPOR1113 - Files not found

Input File	Size	Status	Created Date	Output File
No data available in table				

Showing 0 to 0 of 0 entries

Figure 98: Invalid File Name Format

17. HDT Troubleshooting & Support Information

17.1 Troubleshooting

HDT application hours of operation are determined by CMS policy, support, hardware availability, and availability of required interfaces.

The HDT database will be available during the following time periods:

Monday: 6AM - 11:59PM ET

Tuesday: 6AM - 11:59PM ET

Wednesday: 6AM - 11:59PM ET

Thursday: 6AM - 11:59PM ET

Friday: 6AM - 11:59PM ET

Saturday: 12AM - 11:59PM ET

Sunday: 12AM - 6:59PM, 9PM – 11:59PM ET

Users may be able to login to the HDT application outside these days/times, but the NPI Management functionality will be disabled. If users upload a file to the EFT system using the NPI Batch Management functionality, the batch input file will not be processed until the database becomes available.

If users submit a batch file that does not complete processing before the system becomes unavailable, the batch output file will include an error message that the file could not be processed. The Submitter will need to upload the file again when the HDT database is available.

Scheduled outages for maintenance are communicated to users via email. In addition, MCARE Help Desk support is available Monday through Friday 7:00AM – 7:00PM ET.

17.2 HDT Connectivity Issues

If you experience any problems while using the HDT application, contact the MCARE Help Desk. For contact information for the MCARE Help Desk, refer to section *17.3 Support Information*.

17.3 Support Information

If problems and/or questions arise while accessing the HDT application, contact the MCARE Help Desk at 1-866-324-7315 or at MCARE@cms.hhs.gov Monday through Friday, from 7:00 AM to 7:00 PM ET.

Note: MCARE email is monitored during normal business hours. Emails are typically answered within one business day.

18. HDT Error Messages

18.1 Access and Behavior Error Messages

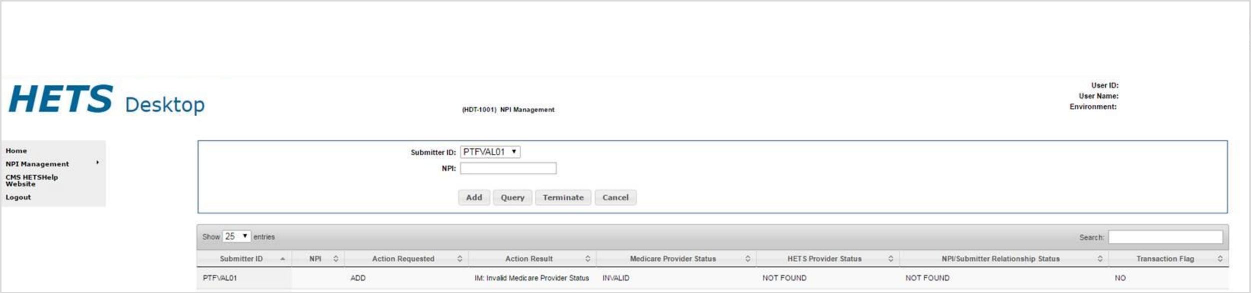
HDT returns a variety of unique errors related to User access or behavior issues. Table 13: Access and Behavior Error Messages provides a complete list of these errors. Each error displays a specific recommendation on screen. Users should follow the on-screen recommendations. When directed to do so, users should take note of the error message they received and then contact the MCARE Help Desk for assistance. For contact information for the MCARE Help Desk, refer to section *17.3 Support Information*.

Table 13: Access and Behavior Error Messages

Error Message
Message 100
Message 110
Message 120
Message 130
Message 700
Message 710
Message 720
Message 730
Message 740
Message 750
Error while processing your request. Please try again.

18.2 Missing or Invalid NPI

On the **NPI Management (HDT-1001)** screen, if users do not enter an NPI number prior to clicking on an action button, or if users enter an invalid NPI format, the NPI Results table will return a response that includes the value entered in the NPI field as well as a Medicare Provider Status of Invalid. Refer to Figure 99: NPI Management – Invalid NPI Screen for an illustration.



Submitter ID: PTFVAL01
NPI:

Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
PTFVAL01		ADD	IM: Invalid Medicare Provider Status	INVALID	NOT FOUND	NOT FOUND	NO

Figure 99: NPI Management – Invalid NPI Screen

18.2.1 Batch File Error Messages

Table 14: Batch File Error Messages identifies the error messages that will be returned in the output file when the input file cannot be processed for the indicated reasons.

Table 14: Batch File Error Messages

Error Message	Condition(s)
Failed to validate file. The file is empty.	The batch file contains no data.
Line #${lineNumber}: Each line must have 3 values: Submitter ID, NPI, and Action	A line in the batch file does not include the 3 requisite elements.
Line #${lineNumber}: Action must be either A, Q, or T	A line in the batch file does not include one of the 3 requisite action code values.
Line #${lineNumber}: Submitter ID length must not exceed 10	A line in the batch file contains a value in the Submitter ID field that is greater than 10 characters.
Line #${lineNumber}: NPI length must be 10. Legacy ID/Source ID is no longer a valid request	A line in the batch file contains a value in the NPI field that is not 10 characters.
Line #${lineNumber}: File could not be processed further.	A line in the batch file cannot be processed.
Line #${lineNumber}: Submitter ID is invalid. File could not be processed further.	The Submitter ID within the file is: Not found, Not associated with the Submitter ID in the file name, Suspended, or Terminated.
A file has already been submitted by Submitter ID ${Submitter ID}. A Submitter can only submit one file in a day.	A Submitter uploads more than one file during a single calendar day using the NPI Batch Management function in HDT.

19. Special Considerations

19.1 Data Size Limits

There is no limit to the NPI Batch Management input file size accepted by the HDT application; however, the EFT file transfer system has a file size limitation of 1GB.

19.2 Daily Batch File Submission

Clearinghouse Submitters are limited to uploading one batch file per day. If a Clearinghouse Submitter attempts to upload more than one file during a single calendar day, an error message is returned in the batch output file.

Appendix A: Record of Changes

Table 15: Record of Changes

Version Number	Date	Description of Change
1.5	3/10/2023	Updated document to reflect updated CMS password policy changes effective in April 2023. Changes include: Section 3, Table 1 updated links Section 5.2, updated to reflect CMS password policy changes including a list of special characters that may be used if the User chooses to include a special character in their 15 character (or more) IDM password Section 7, updated screenshots to reflect changes to CMS password policy
1.4	4/23/2022	Updated Section 14.1 to note that the full HDT URL address is https://HDT.hetsp-haa.cms.gov/HDT/ .
1.3	4/8/2022	Updated Section 14.1 to note that the HDT URL has changed from https://cmshdt.cms.gov/HDT/ to https://HDT.hetsp-haa.cms.gov.
1.2	12/16/2021	Updated Section 4.1 to remove Internet Explorer (IE) from the list of supported internet browsers. Effective January 9th, 2022, CMS Enterprise Portal Services (EPS) no longer supports the IE browser. The EPS landing page will no longer load or be accessible for IE users in the Production environment after January 9, 2022.
1.1	4/23/2021	Updated Section 5.1 to reflect revisions to the HDT policy regarding allowable characters in the IDM User ID or the user’s first and/or last name.
1.0	1/14/2021	Initial draft.

Appendix B: Acronyms

Table 16: Acronyms

Acronym	Literal Translation
CMS	Centers for Medicare & Medicaid Services
EFT	Enterprise File Transfer system
ET	Eastern Time
FFS	Fee For Service
HDT	HETS Desktop
HETS	HIPAA Eligibility Transaction System
HIPAA	Health Insurance Portability and Accountability Act
IDM	Identity Management - also known as the CMS IDM System
IVR	Interactive Voice Response
MCARE	Medicare Customer Assistance Regarding Eligibility
MFA	Multi-factor Authentication
NPI	National Provider Identifier
OTP	One-time Password
PHI	Protected Health Information
QR	Quick Response code
RIDP	Remote Identity Proofing
SMS	Short Message Service
SSN	Social Security Number
UI	User Interface
URL	Uniform Resource Locator

Appendix C: Glossary

Table 17: Glossary

Term	Definition
HETS 270/271 Application	The HETS 270/271 application provides access to Medicare Beneficiary eligibility data in a real-time environment. Submitters may initiate a real-time 270 eligibility request to query coverage information from Medicare on patients for whom services are scheduled or have already been delivered. In real-time mode, the Submitter transmits a 270 request and remains connected while the application processes the transaction and return a 271 response.
HETS Desktop (HDT)	The HETS Desktop (HDT) application is used by HETS 270/271 Submitters to register and maintain an up-to-date record of their business relationships with their Medicare Provider and/or Supplier customers prior to submitting HETS 270/271 transactions. In addition, Submitters are able to verify if NPI numbers are eligible for use with the HETS 270/271 application
HETS Submitter	A Clearinghouse and/or Direct Provider who conducts eligibility transactions via the HETS 270/271 application
HETS Submitter ID	The ID assigned by CMS that allows a Clearinghouse or a Direct Provider to conduct eligibility transactions via the HETS 270/271 application.
User	A person who requires and/or has acquired access to the HDT application.