Centers for Medicare & Medicaid Services

Enterprise Privacy Policy Engine Cloud (EPPE)

Training Module-
User Registration Process

Version 2.0

01/22/2024

Document Number: EPPE-299-IDM-v2.0

Table of Contents

List of Figures

List of Tables

1 Overview

This Training Guide will cover the following:

- EPPE Overview
- IDM Overview
- Multi-Factor Authentication (MFA) Overview
- IDM Registration Process
- EPPE Registration Process
- Experian Identity Verification
- Requesting Access to EPPE
- Requesting Access to EPPE Roles

1.1 EPPE Access Prerequisites

Before continuing this training, please complete the following:

- Obtain Identity Management (IDM) Credentials, Multi-Factor Authentication (MFA), and EPPE Access: https://www.cms.gov/files/document/eppeidm.pdf
- Access CMS Portal: https://portal.cms.gov/

1.2 Icons Used Throughout the EPPE System


A red asterisk denotes that a field is required to be entered.


The question mark icon, when selected, will display field specific help.

2 About EPPE

The Enterprise Privacy Policy Engine (EPPE) system automates the process of submitting Data Use Agreement (DUA) requests and tracking their status through the approval and data receipt stages. End users, (requesters and all CMS approvers), can interactively use the system to manage their DUAs. For those requests that require supporting documentation, it allows documents to be uploaded and then later downloaded for review.

The EPPE Application processes the following 4 DUA Customer Types:

- Contractor
- Limited Data Sets
- Researcher
- Non-DUA Tracking Requests

This training will guide you through the steps necessary to gain access to the EPPE system.

2.1 Identify Management (IDM) Introduction

The IDM system used by EPPE provides users with access to CMS applications. CMS established IDM to provide business partners with a means to create a single User ID that they can use to access one or more CMS applications.

To apply and receive an IDM User ID, complete the steps that follow.

2.2 Multi-Factor Authentication (MFA) Overview

Multi-Factor Authentication (MFA) is generally required to access CMS sensitive data. MFA uses a combination of two (or more) different token attributes (also known as factors), to authenticate the user. The EPPE Application requires two types of authentications.

- The first factor is what users know. This is usually a password, but this can also include a user response to a secret challenge question. (This is generally known as Knowledge Based Authentication, and by itself, is insufficient for authentication to most CMS sensitive information.)
- The second factor is what users have. This could be a physical object (hard token), for example, a smart card, or hardware token that generates one-time-only passwords. It might also be some encrypted software token (soft token) installed on an individual's system (usually with very limited functional parameters for use).

Note: Some MFA options require the installation of an application on a smartphone.

The available MFA Options are listed below:

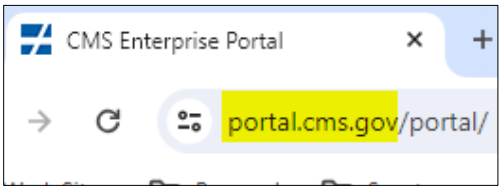
- **Email** – This is the default option that is initially used to access IDM for the first time. Once the user logs in successfully, the user can specify any or all of the other MFA options through a profile update or continue to use email. Email is the only option that cannot be removed and will always remain on your profile.
- **Short Message Service (SMS)** – The SMS option will send your MFA Code directly to your mobile device via a text message. This option requires you to provide a ten-digit U.S. phone number for a mobile device that is capable of receiving text messages. A carrier service charge may apply for this option.

- **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 10-digit U.S. phone number and (optional) extension that will be used during login to obtain the MFA Code.
- **Google Authenticator** – The Google Authenticator is an application for your smart phone that generates security codes. You will be asked for a security code whenever you need to verify your identity. Supported phones include iPhone, Android Phone, and Blackberry (a download to user's smartphone is required).
- **Okta Verify** – The Okta Verify option produces push notifications which enable you to verify your identity with a single tap on your mobile device, without the need to type a code. Supported phones include iPhone, Android Phone, and Windows Phone (a download to user's smartphone is required).

2.3 IDM Registration Process

This step will guide you through creating your IDM profile, which will require both your personal and business-related information.

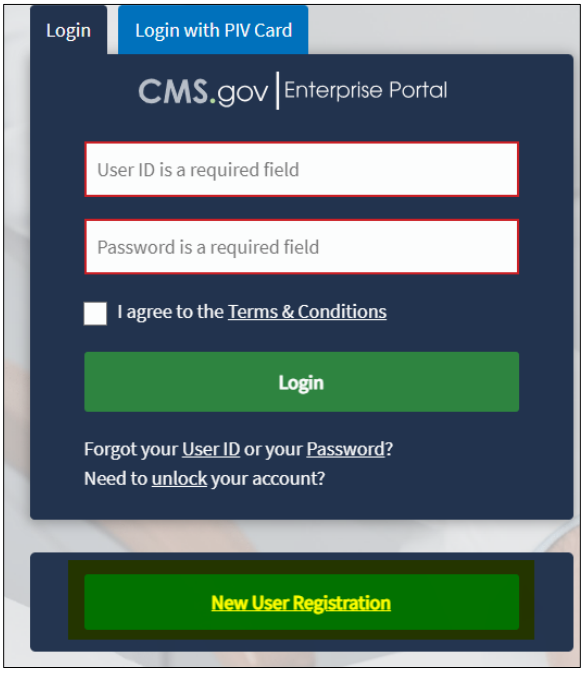
Figure 1: IDM Registration URL Address



1. Navigate to https://portal.cms.gov

The CMS Enterprise Portal is displayed.

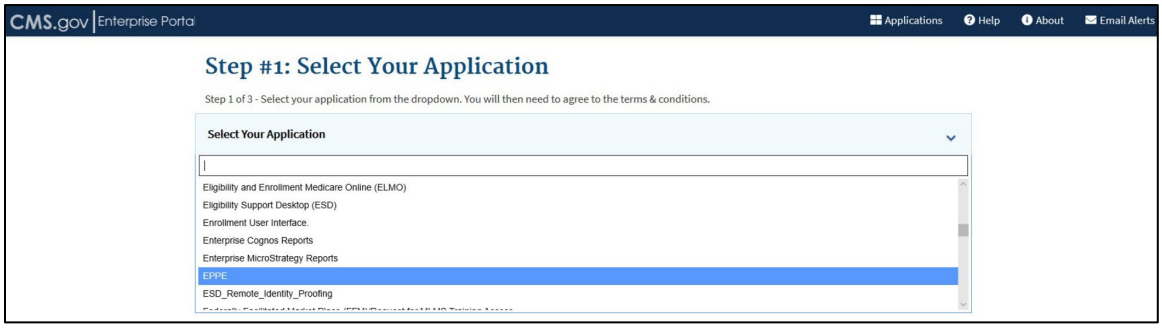
Figure 2: IDM Registration Login Page



1. Click **New User Registration.**

The Select Your Application Page is displayed.

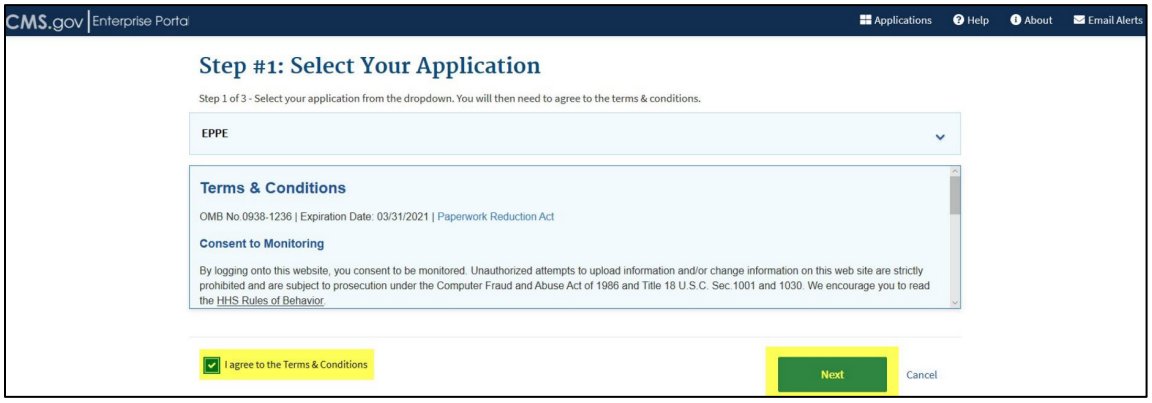
Figure 3: IDM Registration Application Selection



1. Select **EPPE** from the drop-down menu.

The **Terms and Conditions** Page is displayed.

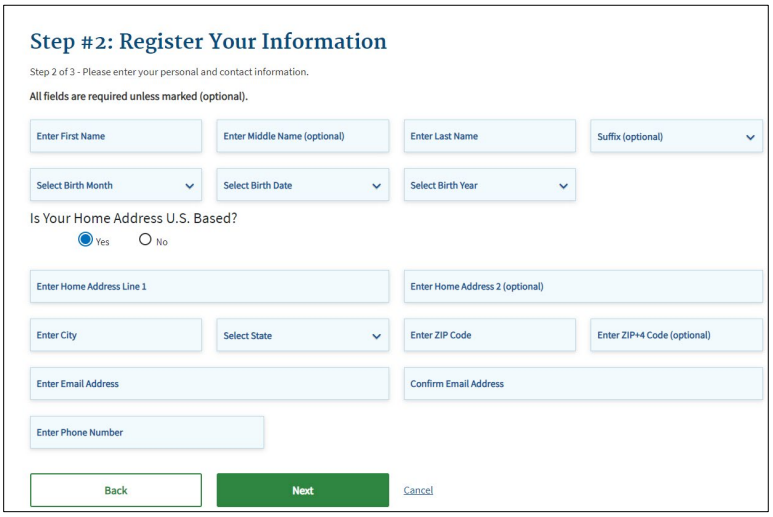
Figure 4: IDM Registration Terms and Conditions



2. Select **I agree to the Terms and Conditions** checkbox.
3. Click **Next.**

The Register Your Information Page is displayed.

Figure 5: IDM Registration Your Information Page

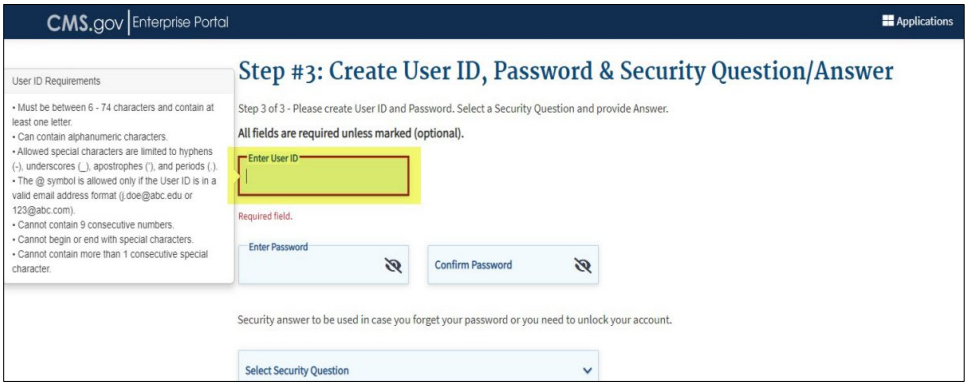


1. Complete all required information.
2. Click **Next.**

Note: Please provide your business email address. All other information provided should be your personal information.

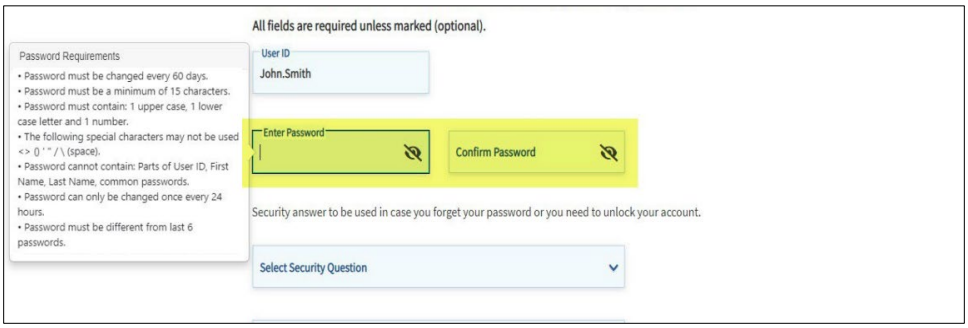
The Create User ID, Password, & Security Question/Answer Page is displayed.

Figure 6: IDM Registration User ID



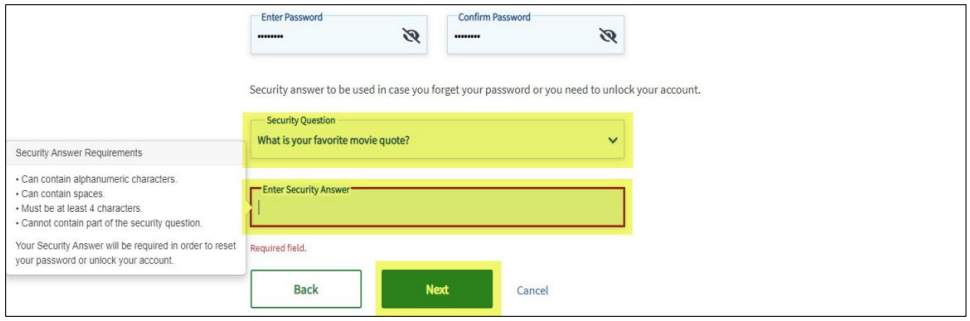
1. Enter **User ID.**

Figure 7: IDM Registration Password



2. Enter **Password.**
3. Re-enter and **Confirm Password.**

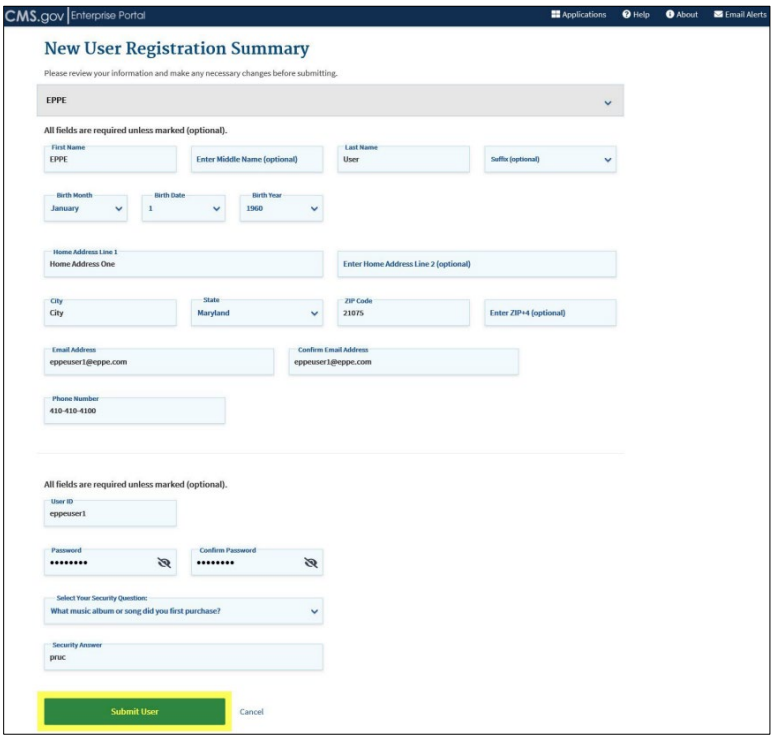
Figure 8: IDM Registration Security Question and Answer



4. Select **Security Question** from the drop-down menu**.**
5. Enter **Security Answer.**
6. Click **Next.**

The New User Registration Summary page is displayed.

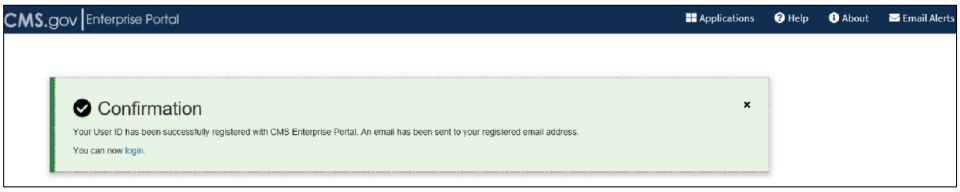
Figure 9: IDM Registration Summary



1. Review the entered information and then click **Submit User.**

A User Registration confirmation message is displayed.

Figure 10: IDM Registration Confirmation



1. The Confirmation Message states '***Your User ID has been successfully registered with CMS Enterprise Portal. An email has been sent to your registered email address. You can now login.***'

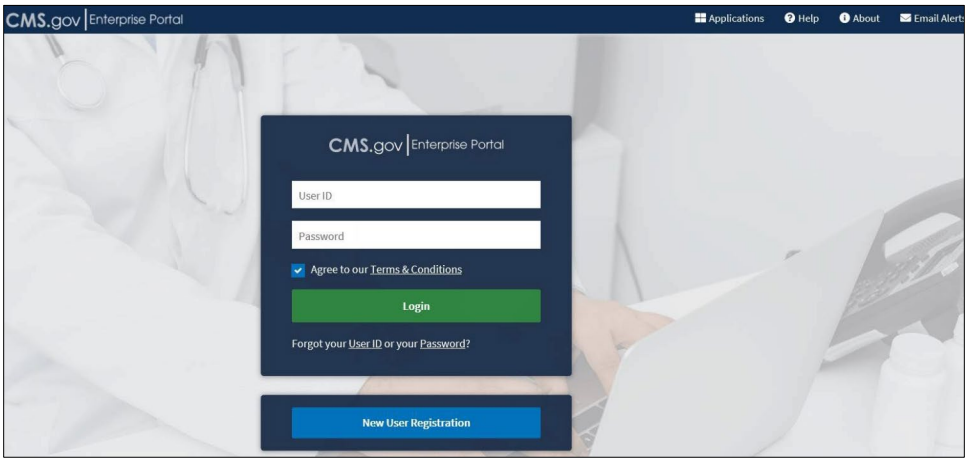
The IDM Registration Process is now complete. You will receive an email notifying you of the successful creation of your account.

2.4 EPPE Registration Process

EPPE is accessible through the CMS Enterprise Portal by using a valid Identity Management (IDM) User ID.

Note: Users must use an IDM User ID, not an Enterprise User Administration (EUA) User ID, to access the EPPE application.

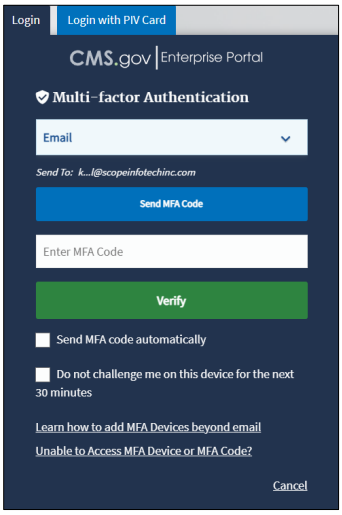
Figure 11: Requesting Access Login Page



2. Enter **User ID and Password.**
3. Click the **Agree to our Terms & Conditions** checkbox.
4. Click **Login.**

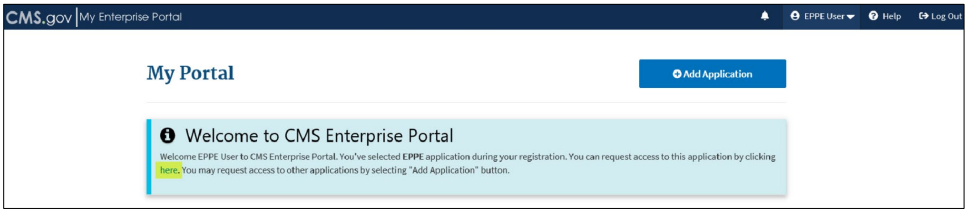
Multi-Factor Authentication is displayed.

Figure 12: Requesting Access Multi-Factor Authentication



1. Enter **Multi-Factor Authentication Code.**
2. Click **Verify.**

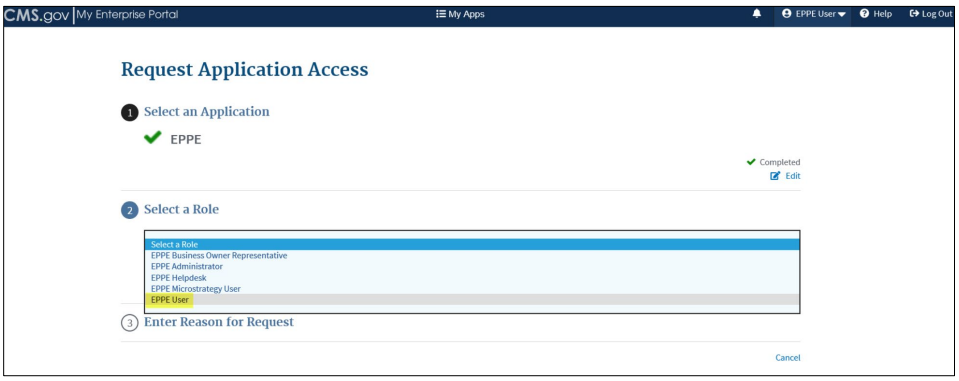
Figure 13: Requesting Access My Portal



1. Click on "**here**" to request access to the EPPE application.

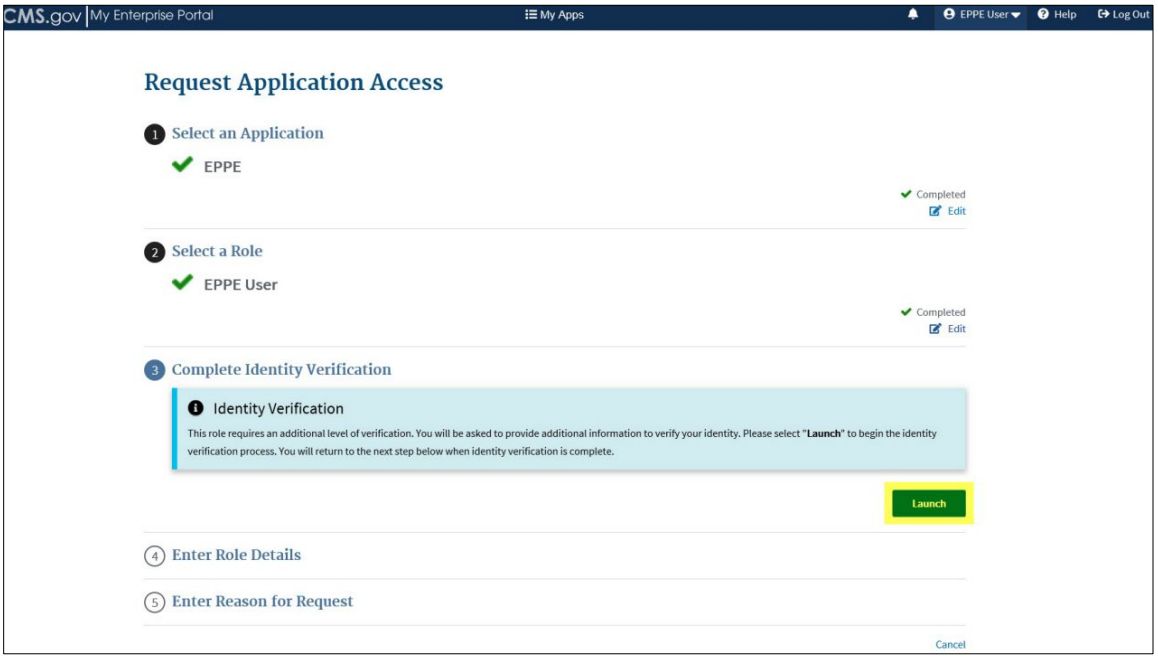
The Request Application Access Page is displayed.

Figure 14: Requesting Access Role Selection



2. The **Select an Application** field is populated by default.
3. Click the **Select a Role** field and choose **EPPE User** from the drop-down menu.
4. Click **Next.**

Figure 15: Requesting Access Identity Verification



5. Click **Launch** to start the **Identity Verification** process.

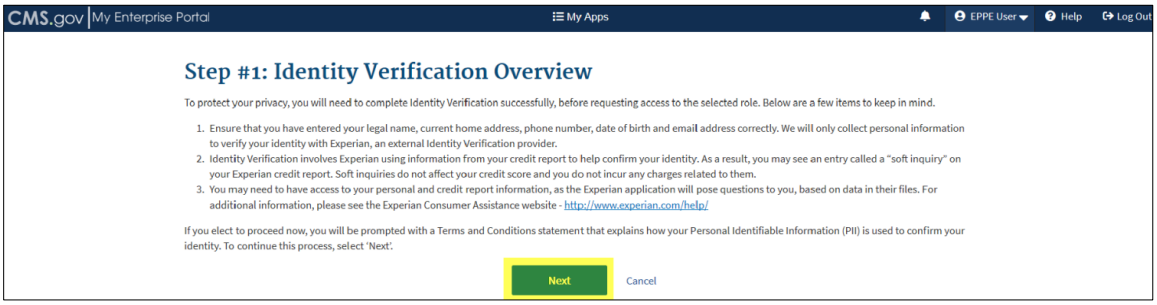
2.5 Experian Identity Verification

The Experian identity verification service will use the user's core credentials to locate their personal information in Experian and generate a set of questions, referred to as out-of-wallet questions. Experian will attempt to verify their identity to the appropriate level of assurance with the information they provided. Most users are able to complete the ID proofing process in less than five minutes. If users encounter problems with RIDP, they will be asked to contact Experian Support Services via phone to resolve any issues. The Experian identity verification is a required step to access the EPPE system and must be completed.

Users may have already encountered Remote Identity Proofing (RIDP) through various interactions with banking systems, credit reporting agencies, and shipping companies. The Experian identity verification service is used by CMS to confirm your identity when users access a protected CMS Application. When users log into the CMS system and request access to EPPE, they will be prompted to RIDP if they have not been previously identity proofed to the level of assurance required by the EPPE application. RIDP will not impact the user's credit. Users will be asked to provide a set of core credentials which include:

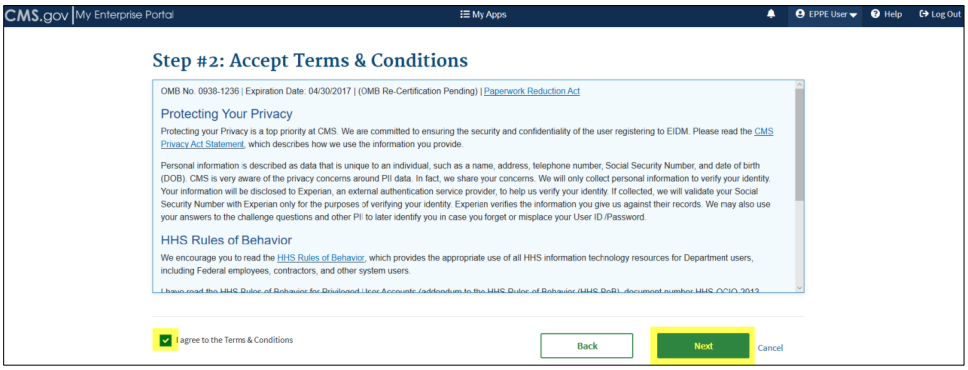
1. Full Legal Name
2. Social Security Number
3. Date of Birth
4. Current Residential Address
5. Personal Phone Number

Figure 16: Identity Verification Step 1



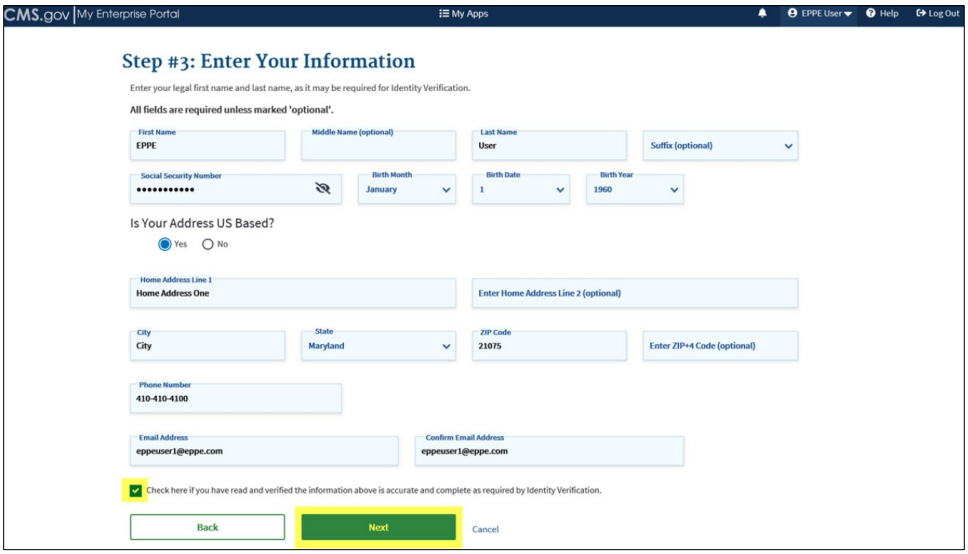
1. Click **Next.**

Figure 17: Identity Verification Step 2



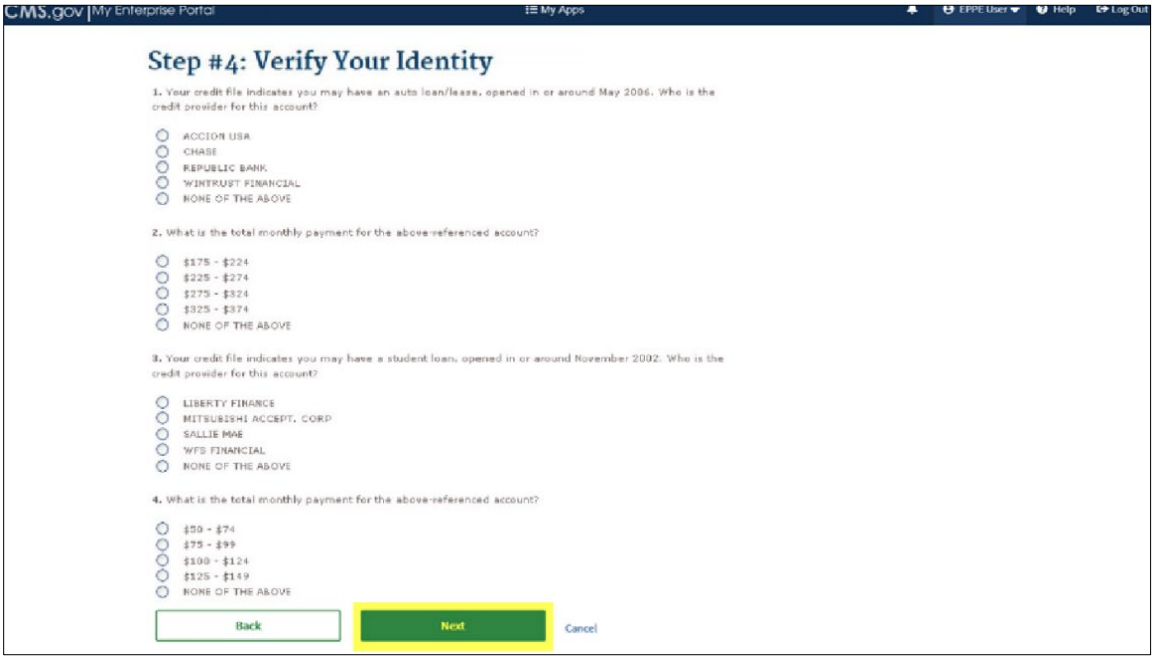
1. Click the **I agree to the Terms & Conditions** checkbox.
2. Click **Next.**

Figure 18: Identity Verification Step 3



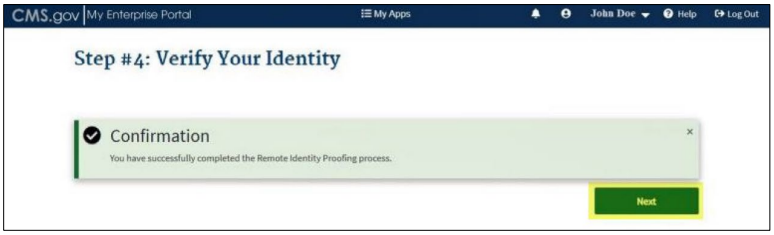
1. Click the **Check here if you have read and verified the information above is accurate and complete as required by Identity Verification** checkbox.
2. Click **Next.**

Figure 19: Identity Verification Step 4



1. Provide an answer to each question and then click **Next.**

Figure 20: Identity Verification Confirmation

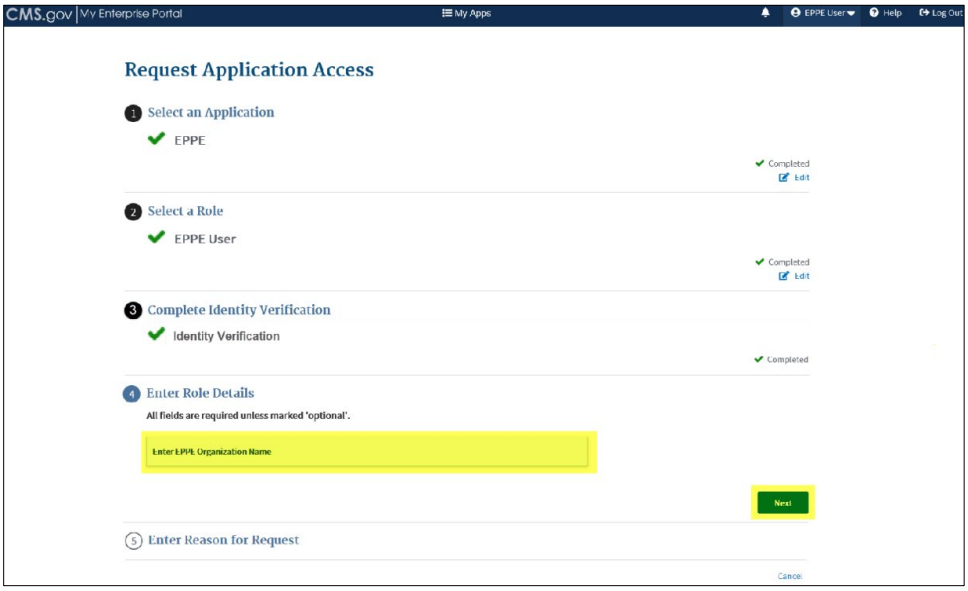


2. The confirmation message, "**You have successfully completed the Remote Identity Proofing process**" displays.
3. Click **Next**.

2.6 Requesting Access to EPPE

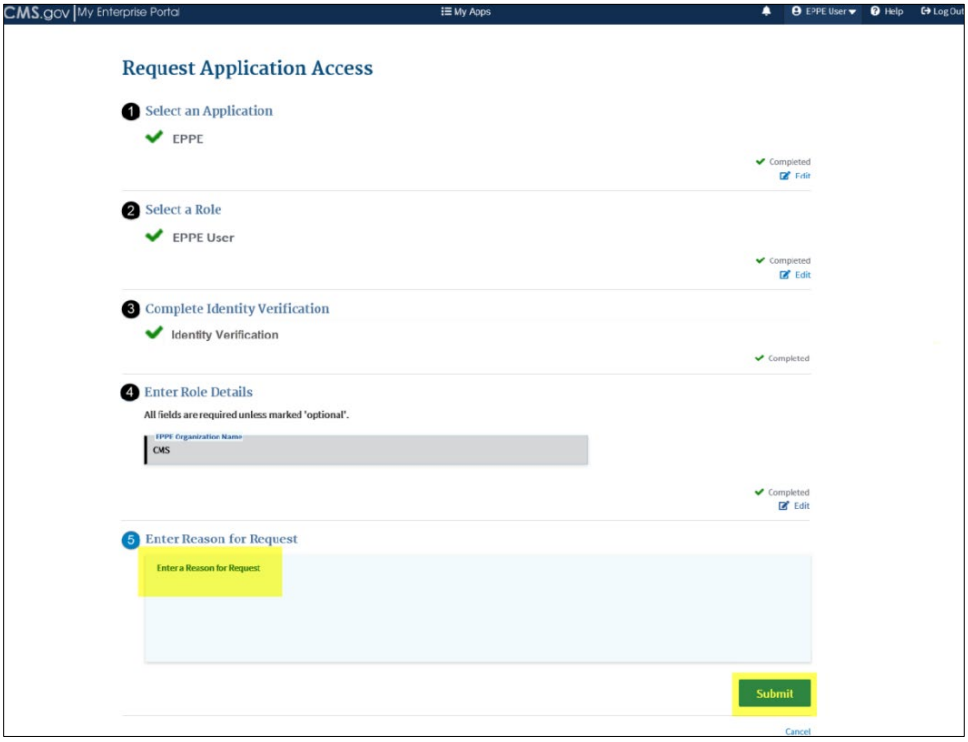
Requesting Access to EPPE is accessible when the Identification Verification is complete.

Figure 21: Requesting Access Role Details



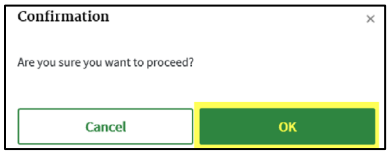
1. Enter the **Organization Name.**
2. Click **Next.**

Figure 22: Requesting Access Reason for Request



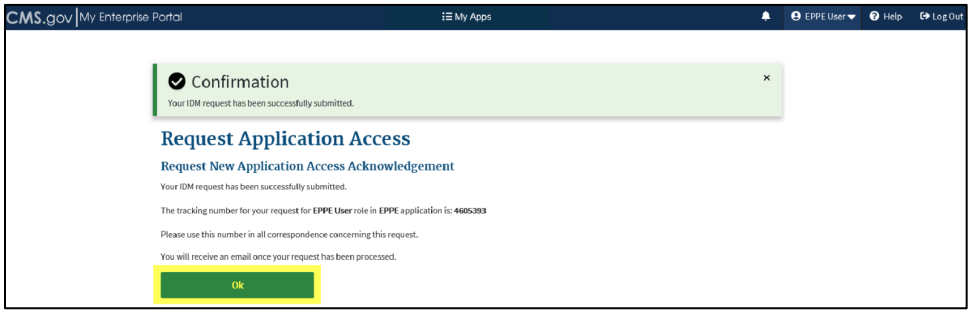
1. Enter the **Reason for Request.**
2. Click **Submit.**

Figure 23: Requesting Access Confirmation Request



1. Click **OK** to proceed.

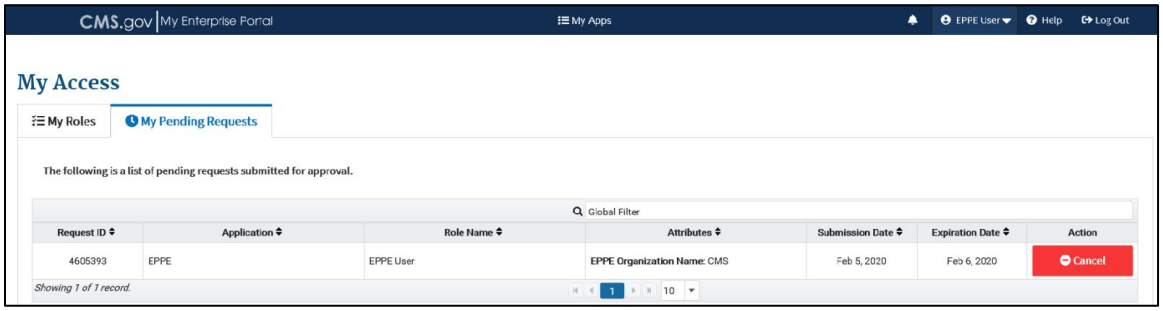
Figure 24: Requesting Access Confirmation Message



2. Click **OK** to return to the Enterprise Poral page.

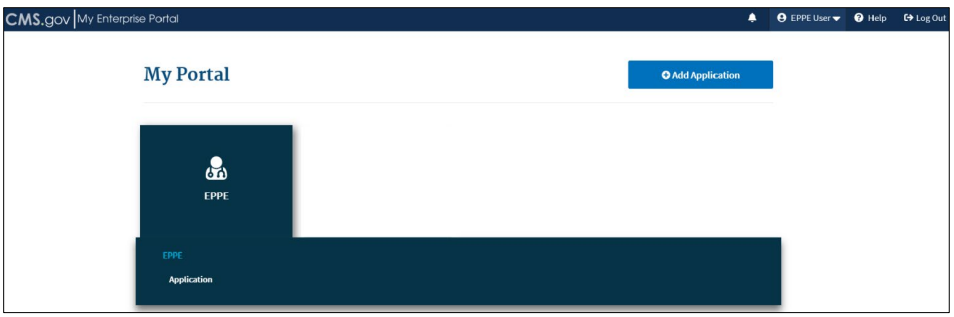
2.7 Requesting Access to EPPE Roles

Figure 25: Requesting Access My Access Page



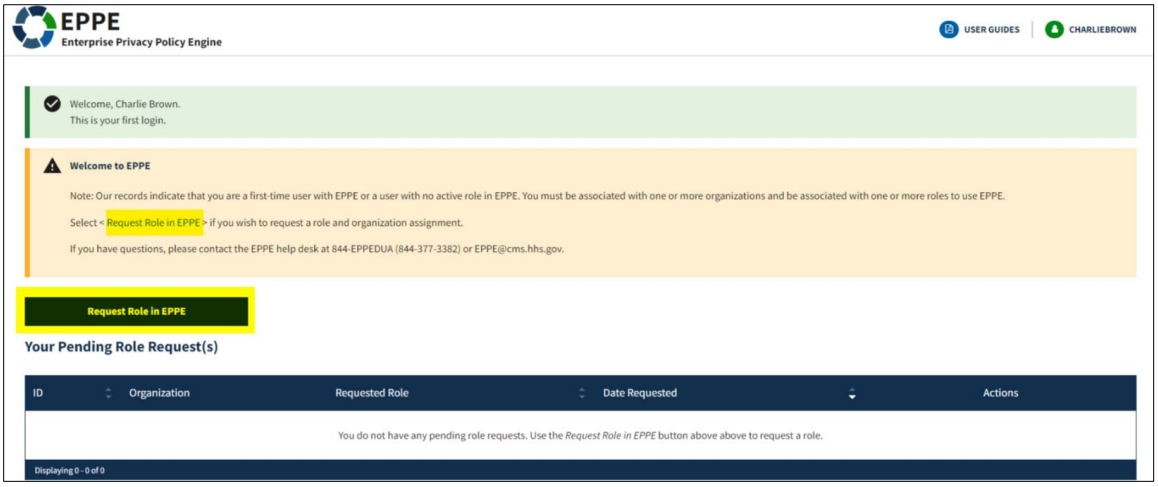
At this point the Application Access Request is complete. The request must be approved. An email will be sent once the pending request is approved. After access is granted, log into the Enterprise Portal.

Figure 26: Requesting an EPPE Role My Portal Page



1. Click on the **EPPE** tile.
2. Then click on the **Application** link.

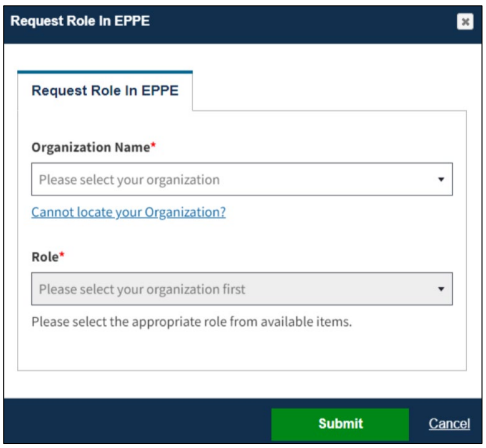
Figure 27: Requesting an EPPE Role EPPE First Time User Page



1. Click on the **Request a Role in EPPE** hyperlink or button.

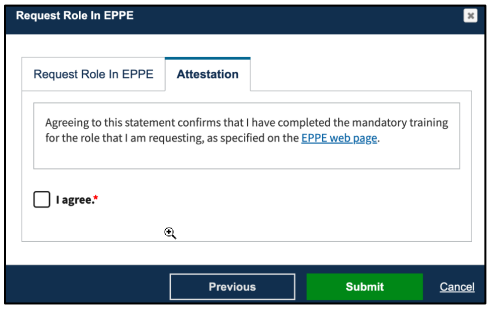
The Request a Role in EPPE pop-out window is displayed.

Figure 28: Requesting an EPPE Role Request a Role in EPPE Pop-Out Window



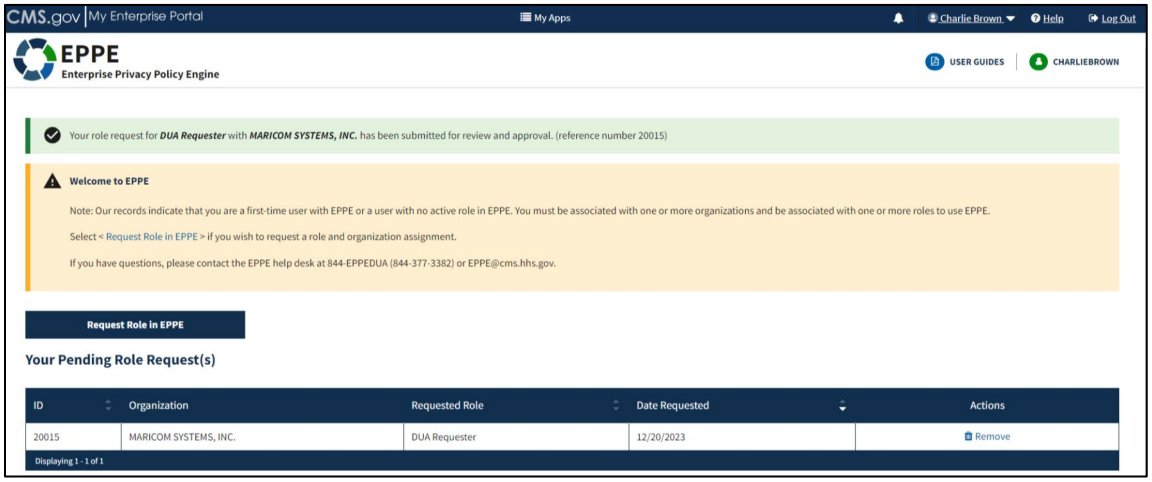
2. Select an **Organization** from the drop-down menu.
3. Select a **Role** from the drop-down menu.
4. Click **Submit.**

Figure 29: EPPE Role Request Attestation.



2. Click the **I agree** checkbox.

Figure 30: Requesting an EPPE Role Confirmation.



1. The EPPE role request submission acknowledgement displays the message, "**Your organization/role request has been submitted for approval**."
2. The EPPE Administrator will review for approval.

3 Acronyms and Glossary

The following are acronyms used within the EPPE system.

Table 1: Acronyms

Acronym	Definition
CMS	Centers for Medicare and Medicaid Services
DUA	Data Use Agreement
EPPE	Enterprise Privacy Policy Engine
IDM	Identity Management
MFA	Multi-Factor Authentication
PDF	Portable Document Format

4 EPPE Help Desk Information

EPPE Help Desk Contact Information

Hours of Operation: Monday – Friday 9:00 AM to 6:00 PM EST

844-EPPE-DUA (844-377-3382)

eppe@cms.hhs.gov