



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

| | |
|--|-----------|
| 1 Overview | 1 |
| 1.1 EPPE Access Prerequisites | 1 |
| 1.2 Icons Used Throughout the EPPE System | 1 |
| 2 About EPPE | 2 |
| 2.1 Identify Management (IDM) Introduction..... | 2 |
| 2.2 Multi-Factor Authentication (MFA) Overview | 2 |
| 2.3 IDM Registration Process | 3 |
| 2.4 EPPE Registration Process | 7 |
| 2.5 Experian Identity Verification | 9 |
| 2.6 Requesting Access to EPPE..... | 11 |
| 2.7 Requesting Access to EPPE Roles..... | 13 |
| 3 Acronyms and Glossary | 16 |
| 4 EPPE Help Desk Information | 17 |

List of Figures

| | |
|--|----|
| Figure 1: IDM Registration URL Address | 3 |
| Figure 2: IDM Registration Login Page | 3 |
| Figure 3: IDM Registration Application Selection | 4 |
| Figure 4: IDM Registration Terms and Conditions | 4 |
| Figure 5: IDM Registration Your Information Page..... | 5 |
| Figure 6: IDM Registration User ID | 5 |
| Figure 7: IDM Registration Password..... | 5 |
| Figure 8: IDM Registration Security Question and Answer | 6 |
| Figure 9: IDM Registration Summary | 6 |
| Figure 10: IDM Registration Confirmation | 7 |
| Figure 11: Requesting Access Login Page | 7 |
| Figure 12: Requesting Access Multi-Factor Authentication | 8 |
| Figure 13: Requesting Access My Portal | 8 |
| Figure 14: Requesting Access Role Selection | 8 |
| Figure 15: Requesting Access Identity Verification | 9 |
| Figure 16: Identity Verification Step 1..... | 10 |
| Figure 17: Identity Verification Step 2..... | 10 |

| | |
|--|----|
| Figure 18: Identity Verification Step 3..... | 10 |
| Figure 19: Identity Verification Step 4..... | 11 |
| Figure 20: Identity Verification Confirmation..... | 11 |
| Figure 21: Requesting Access Role Details | 12 |
| Figure 22: Requesting Access Reason for Request..... | 12 |
| Figure 23: Requesting Access Confirmation Request | 13 |
| Figure 24: Requesting Access Confirmation Message..... | 13 |
| Figure 25: Requesting Access My Access Page | 13 |
| Figure 26: Requesting an EPPE Role My Portal Page..... | 13 |
| Figure 27: Requesting an EPPE Role EPPE First Time User Page | 14 |
| Figure 28: Requesting an EPPE Role Request a Role in EPPE Pop-Out Window | 14 |
| Figure 29: EPPE Role Request Attestation. | 15 |
| Figure 30: Requesting an EPPE Role Confirmation..... | 15 |

List of Tables

| | |
|-------------------------|----|
| Table 1: Acronyms | 16 |
|-------------------------|----|

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:

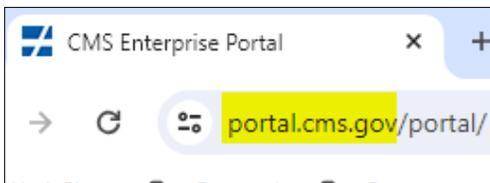
- **Email** – This is the default option that is initially used to access IDM for the first time. Once the user logs in successfully, the user can specify any or all of the other MFA options through a profile update or continue to use email. Email is the only option that cannot be removed and will always 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.

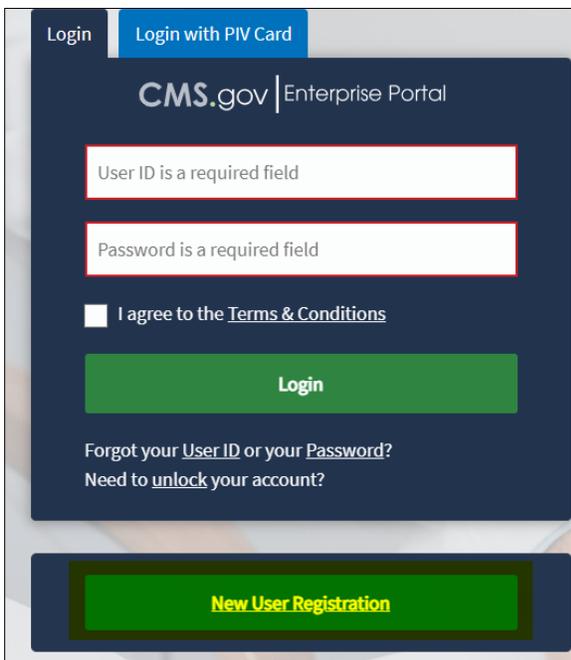
Figure 1: IDM Registration URL Address



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

The CMS Enterprise Portal is displayed.

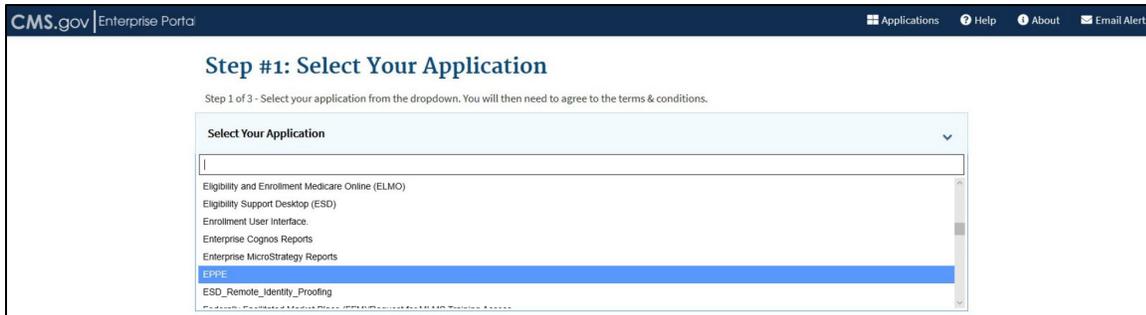
Figure 2: IDM Registration Login Page



1. Click **New User Registration**.

The Select Your Application Page is displayed.

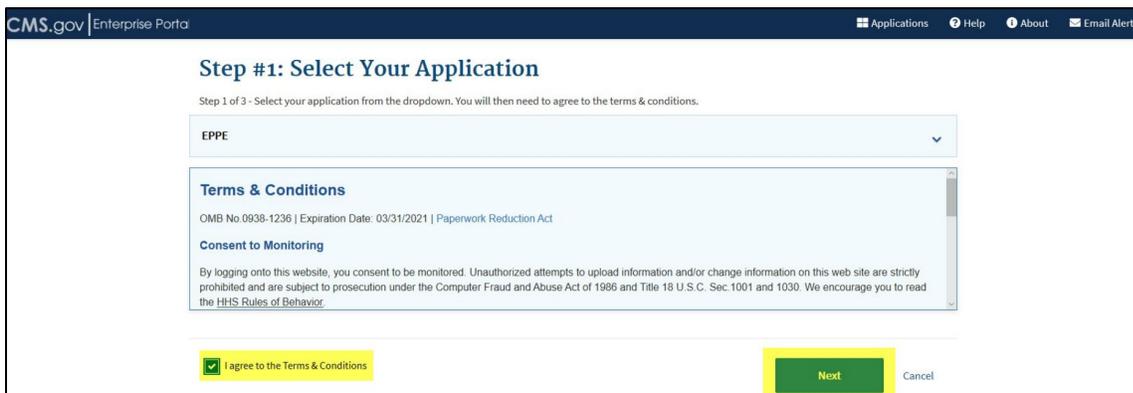
Figure 3: IDM Registration Application Selection



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

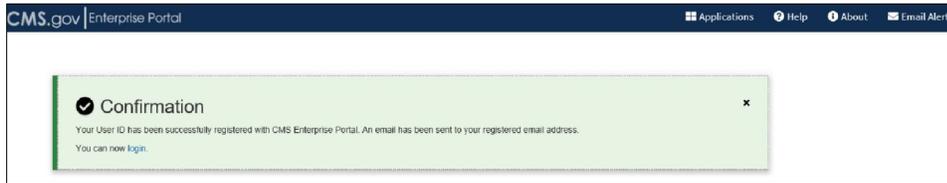
4. Select **Security Question** from the drop-down menu.
5. Enter **Security Answer**.
6. Click **Next**.

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

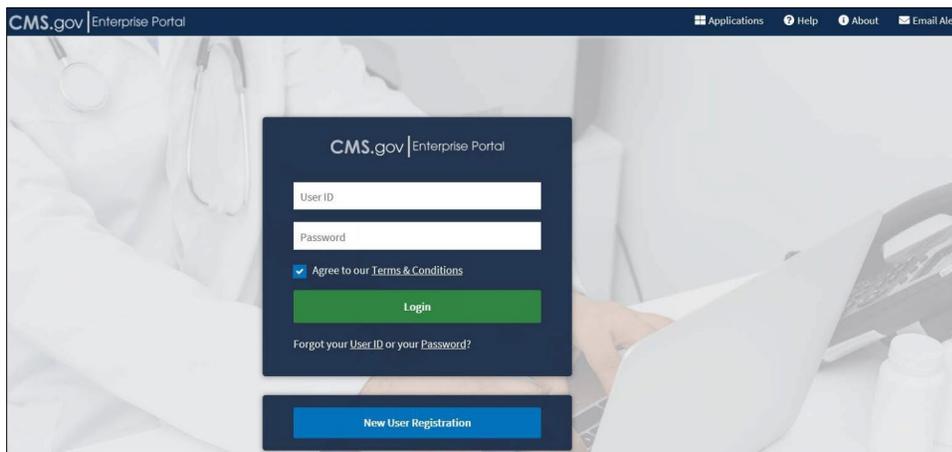
1. The Confirmation Message states '***Your User ID has been successfully registered with CMS Enterprise Portal. An email has been sent to your registered email address. You can now login.***

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.

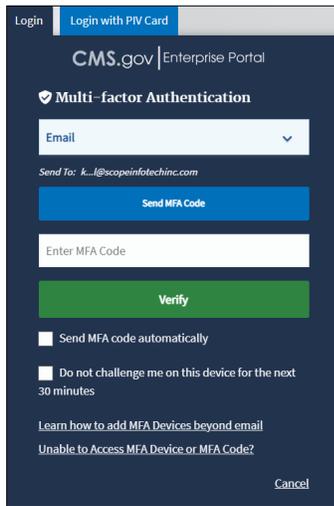
Note: Users must use an IDM User ID, not an Enterprise User Administration (EUA) User ID, to access the EPPE application.

Figure 11: Requesting Access Login Page

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

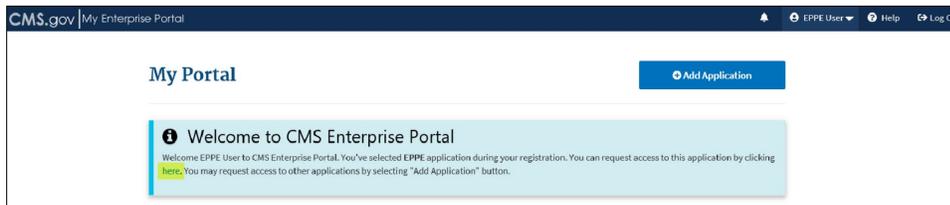
Multi-Factor Authentication is displayed.

Figure 12: Requesting Access Multi-Factor Authentication



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

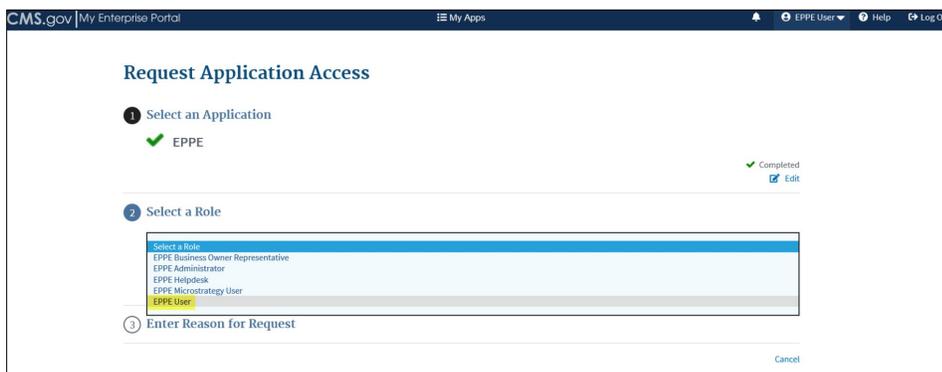
Figure 13: Requesting Access My Portal



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

The screenshot shows the 'Request Application Access' page in the CMS.gov My Enterprise Portal. The page is titled 'Request Application Access' and features a progress bar with five steps:

- 1 Select an Application**: A green checkmark indicates completion. The application 'EPPE' is selected. A 'Completed' status and an 'Edit' link are visible.
- 2 Select a Role**: A green checkmark indicates completion. The role 'EPPE User' is selected. A 'Completed' status and an 'Edit' link are visible.
- 3 Complete Identity Verification**: This step is currently active. It contains a sub-step '1 Identity Verification' with a light blue background. The text reads: 'This role requires an additional level of verification. You will be asked to provide additional information to verify your identity. Please select "Launch" to begin the identity verification process. You will return to the next step below when identity verification is complete.' A yellow 'Launch' button is highlighted at the bottom right of this section.
- 4 Enter Role Details**: This step is not yet completed.
- 5 Enter Reason for Request**: This step is not yet completed.

At the bottom right of the page, there is a 'Cancel' link.

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

CMS.gov | My Enterprise Portal

My Apps

EPPE User Help Log Out

Step #4: Verify Your Identity

1. Your credit file indicates you may have an auto loan/lease, opened in or around May 2006. Who is the credit provider for this account?

ACCION USA
 CHASE
 REPUBLIC BANK
 WINTRUST FINANCIAL
 NONE OF THE ABOVE

2. What is the total monthly payment for the above-referenced account?

\$175 - \$224
 \$225 - \$274
 \$275 - \$324
 \$325 - \$374
 NONE OF THE ABOVE

3. Your credit file indicates you may have a student loan, opened in or around November 2002. Who is the credit provider for this account?

LIBERTY FINANCE
 MITSUBISHI ACCEPT. CORP
 SALLIE MAE
 WFS FINANCIAL
 NONE OF THE ABOVE

4. What is the total monthly payment for the above-referenced account?

\$50 - \$74
 \$75 - \$99
 \$100 - \$124
 \$125 - \$149
 NONE OF THE ABOVE

Back Next Cancel

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

Figure 20: Identity Verification Confirmation

CMS.gov | My Enterprise Portal

My Apps John Doe Help Log Out

Step #4: Verify Your Identity

Confirmation
 You have successfully completed the Remote Identity Proofing process.

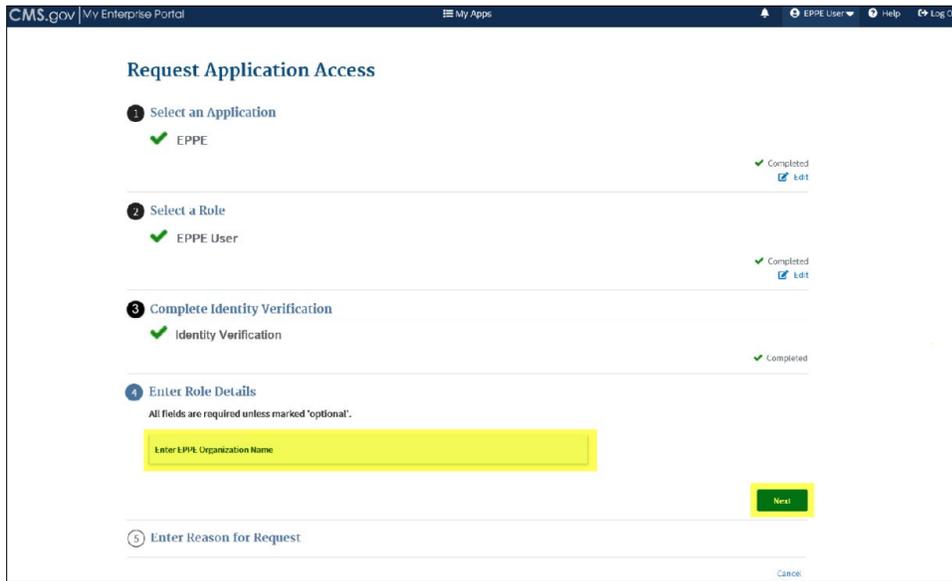
Next

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

2.6 Requesting Access to EPPE

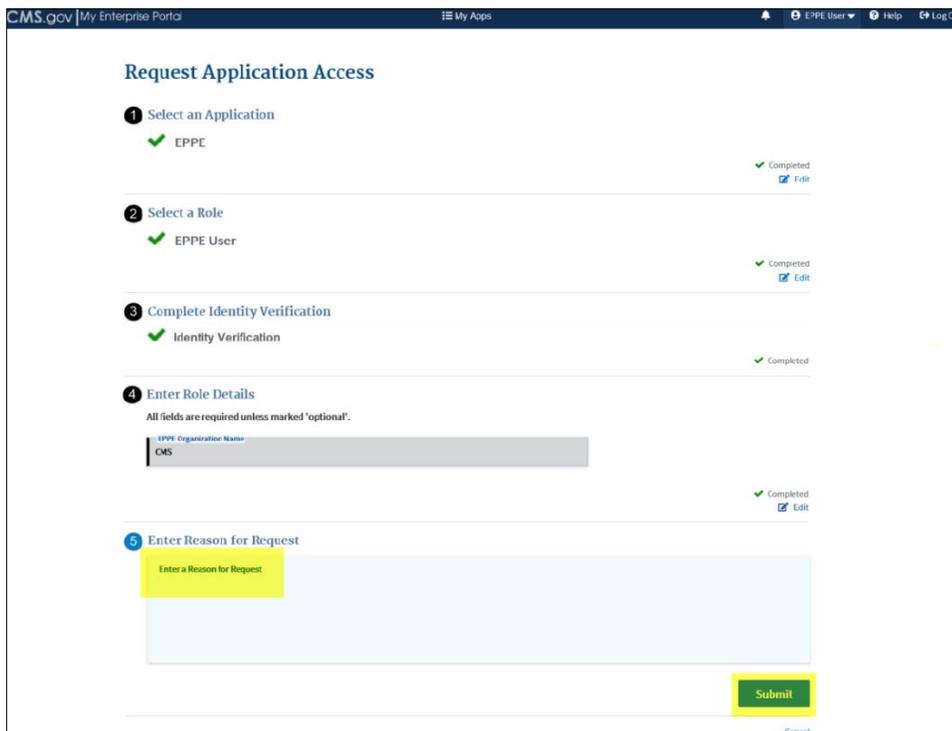
Requesting Access to EPPE is accessible when the Identification Verification is complete.

Figure 21: Requesting Access Role Details



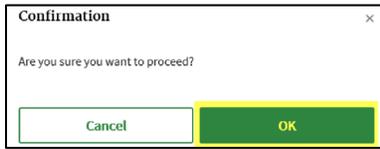
1. Enter the **Organization Name**.
2. Click **Next**.

Figure 22: Requesting Access Reason for Request



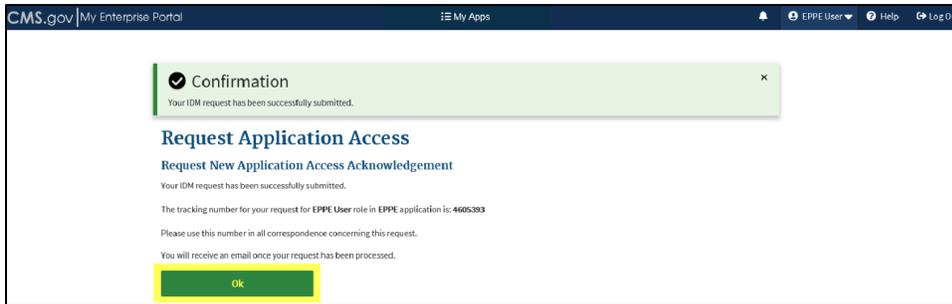
1. Enter the **Reason for Request**.
2. Click **Submit**.

Figure 23: Requesting Access Confirmation Request



1. Click **OK** to proceed.

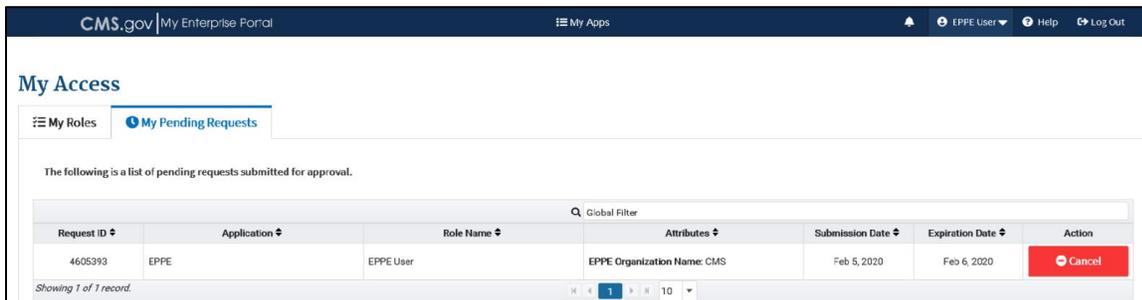
Figure 24: Requesting Access Confirmation Message



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

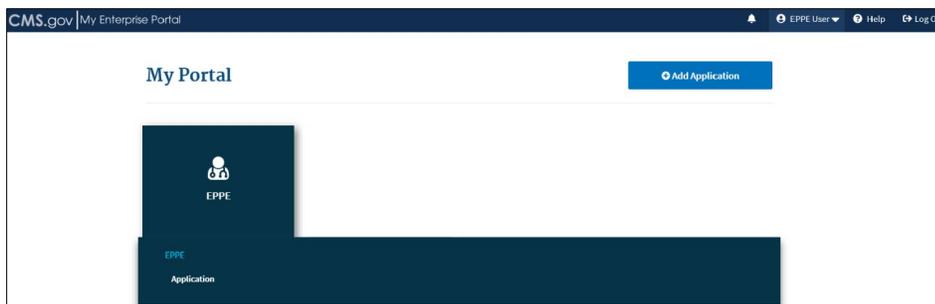
2.7 Requesting Access to EPPE Roles

Figure 25: Requesting Access My Access Page



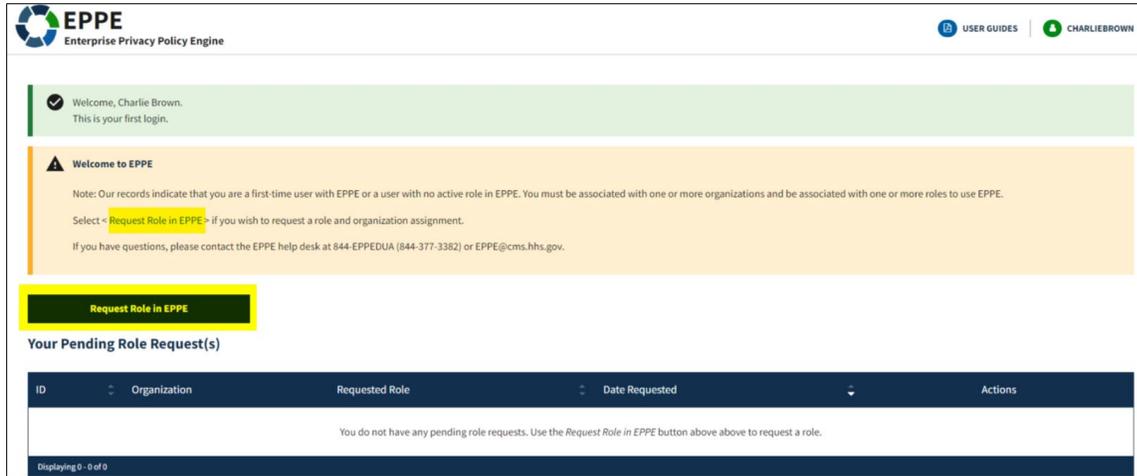
At this point the Application Access Request is complete. The request must be approved. An email will be sent once the pending request is approved. After access is granted, log into the Enterprise Portal.

Figure 26: Requesting an EPPE Role My Portal Page



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

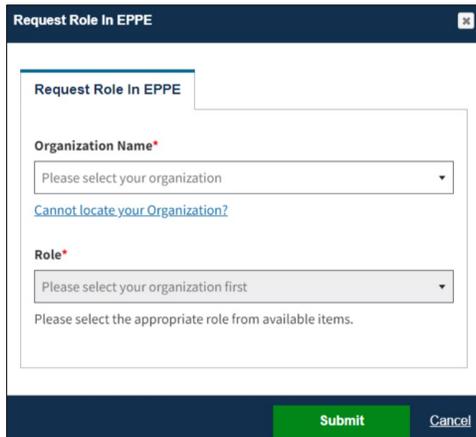
Figure 27: Requesting an EPPE Role EPPE First Time User Page



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.

Request Role In EPPE

Request Role In EPPE **Attestation**

Agreeing to this statement confirms that I have completed the mandatory training for the role that I am requesting, as specified on the [EPPE web page](#).

I agree.*

Previous **Submit** Cancel

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

Figure 30: Requesting an EPPE Role Confirmation.

CMS.gov | My Enterprise Portal My Apps Charlie Brown Help Log Out

EPPE
Enterprise Privacy Policy Engine USER GUIDES CHARLIEBROWN

✔ Your role request for *DUA Requester* with *MARICOM SYSTEMS, INC.* has been submitted for review and approval. (reference number 20015)

⚠ **Welcome to EPPE**

Note: Our records indicate that you are a first-time user with EPPE or a user with no active role in EPPE. You must be associated with one or more organizations and be associated with one or more roles to use EPPE.

Select < Request Role in EPPE > if you wish to request a role and organization assignment.

If you have questions, please contact the EPPE help desk at 844-EPPE-DUA (844-377-3382) or EPPE@cms.hhs.gov.

Request Role in EPPE

Your Pending Role Request(s)

| ID | Organization | Requested Role | Date Requested | Actions |
|-------|-----------------------|----------------|----------------|---------|
| 20015 | MARICOM SYSTEMS, INC. | DUA Requester | 12/20/2023 | Remove |

Displaying 1 - 1 of 1

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