

## My EPP Two-Factor Authentication FAQs

### **What are the minimum technology requirements required for Two-Factor Authentication?**

The minimum technology requirements for using two-factor authentication is either of the following:

1. A device capable of receiving text messages.
2. A device capable of running an authentication application.

### **How do I validate my email address and establish two-factor authentication?**

1. Visit the [NFC Home page](#) and select the My EPP icon from the application launch pad.
2. View/read the warning page and select "I agree" to access the My EPP log in page.

### **If you use eAuthentication to log into My EPP:**

1. Select the eAuth log in button. You will be redirected to the eAuthentication Log In page. You may be prompted to select your Agency before being prompted to sign in to eAuth. PIV is required for all eAuth-enabled Agencies, but you may still have the capability to log in with your username and password.

2. Once logged in, you will be prompted to create a user ID and password.

myEPP

Sample Page

### Security Measures for Your Employee Personal Page

Items marked with an asterisk \* are required.

#### User Id

You are required to establish a new User ID which will replace your Social Security Number when logging on to EPP.

Your User Id

- must be 8-40 characters long and contain at least one letter.
- may contain numbers and special characters !#\$%\*+.-@.
- cannot match your current password.
- cannot contain your SSN.
- cannot contain spaces.

\* New User Id

\* Confirm New User Id

#### Password

Enter a new password below. You must use this new Password for all subsequent logins.

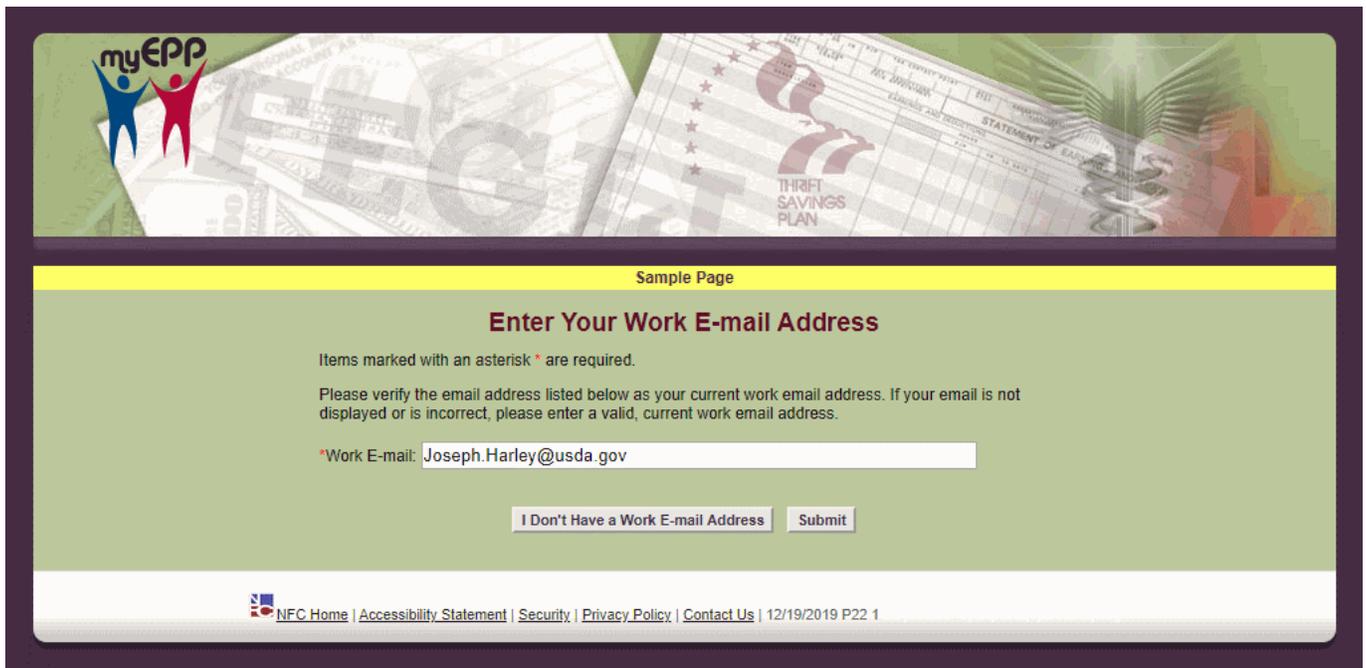
Your Password

- must be 12 to 32 characters,
- must contain at least one character from the 4 following categories:
  - English upper case letters (A-Z)
  - English lower case letters (a-z)
  - Westernized Arabic numerals (0-9)
  - Special characters limited to: ! # \$ % \* \_ +
- cannot contain your first name, last name, User ID, or Ssn,
- cannot match your current or two prior passwords.
- at least 5 characters must be changed.

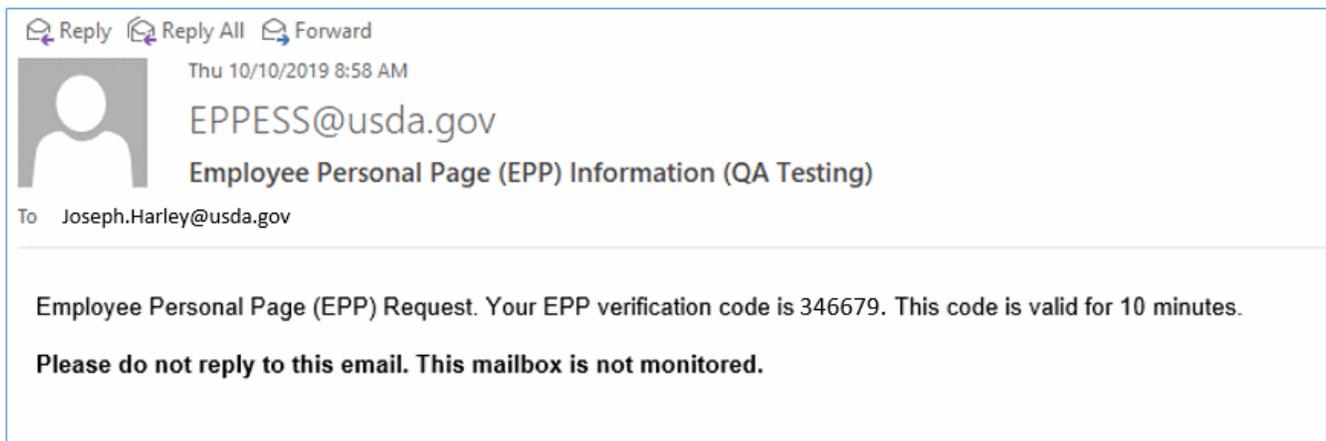
\* New Password

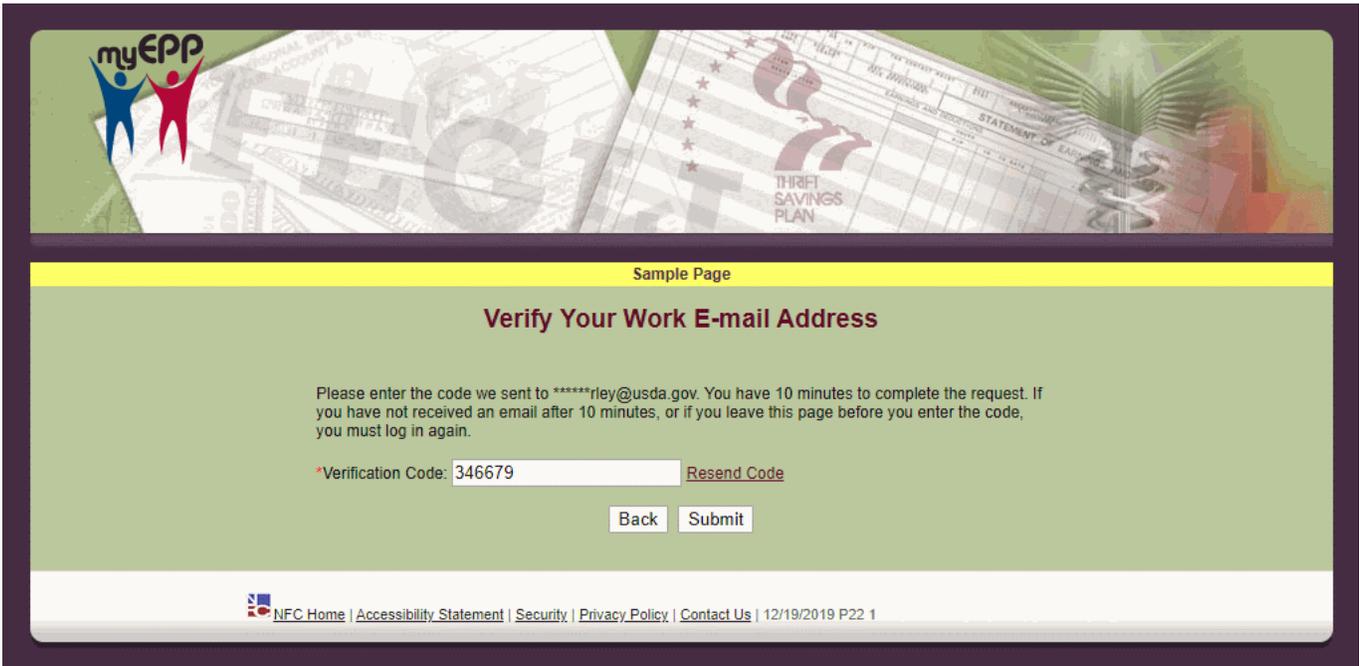
\* Confirm New Password

3. After establishing your user ID and password, you will be prompted to enter or edit your work email address. If you do not have a work email address, please select "I Don't Have a Work Email Address."

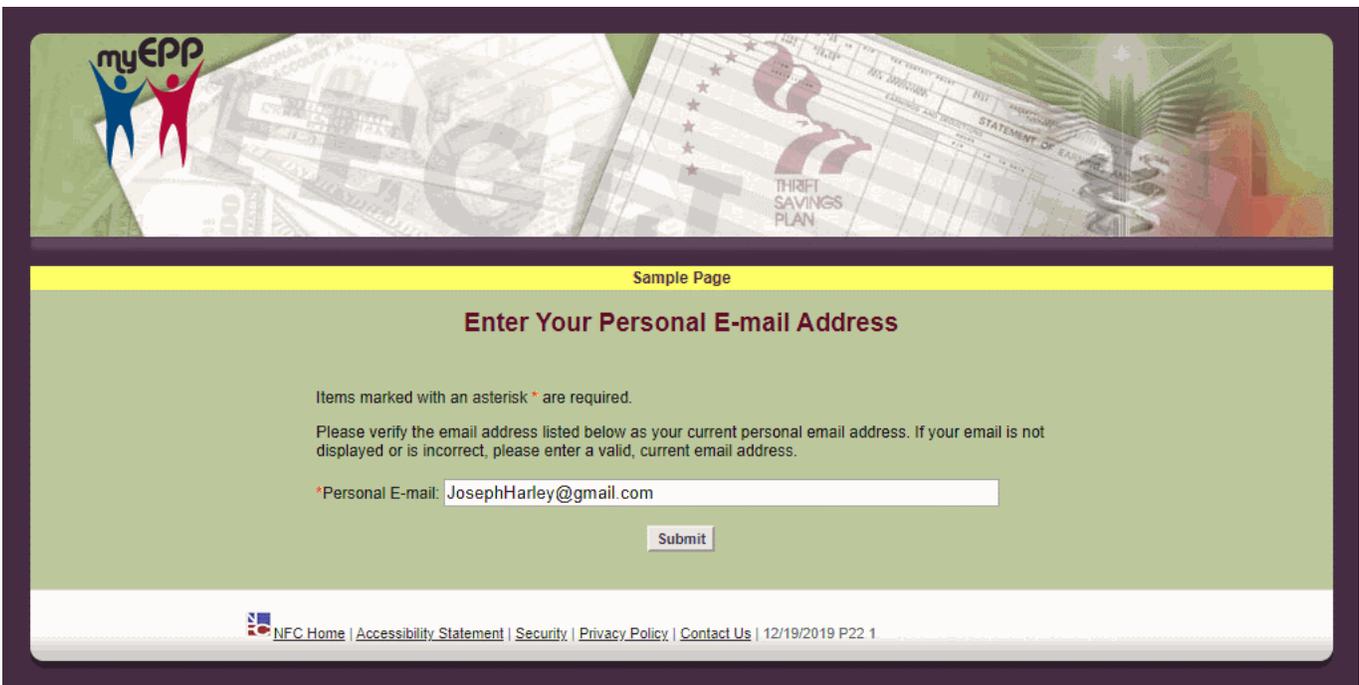


4. You will receive an email via your work email address that contains a verification code. Enter the verification code into My EPP.

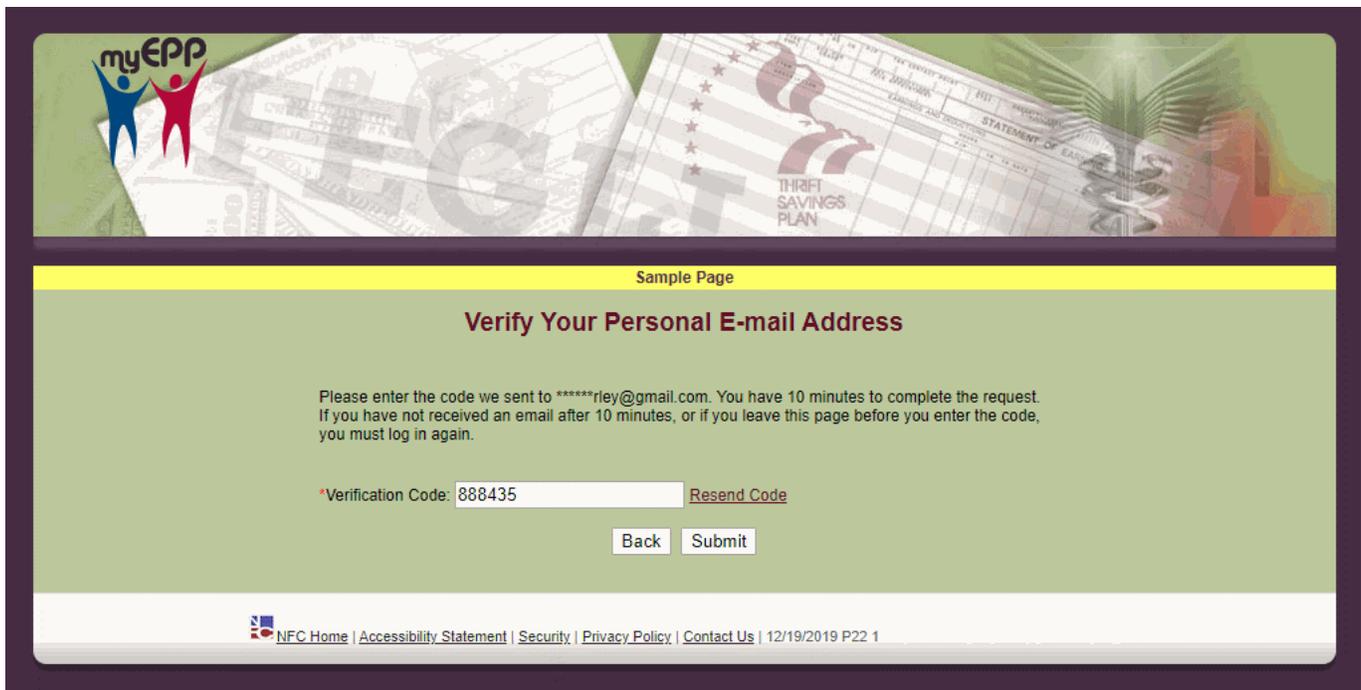
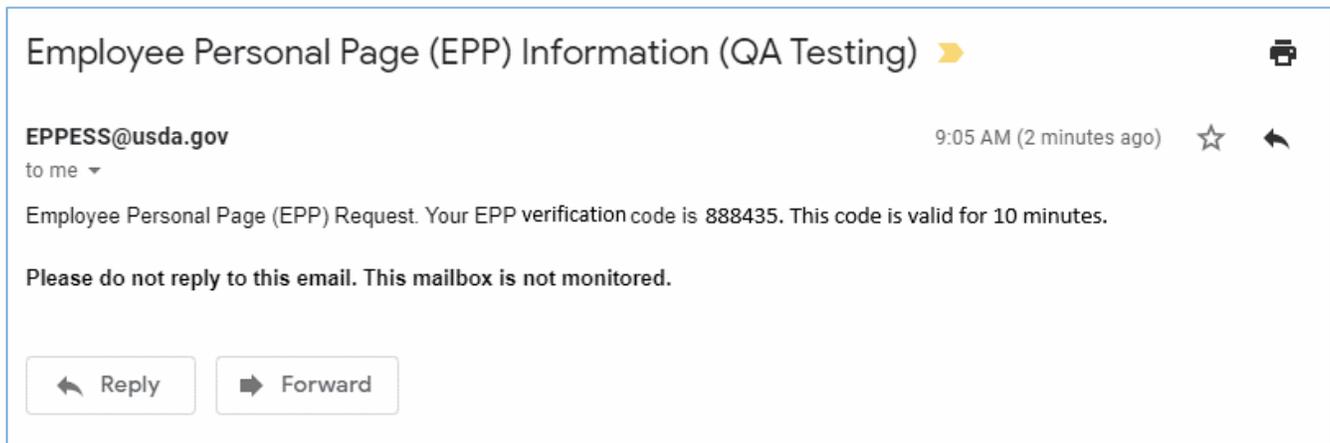




5. After verifying your work email address, you will be prompted to enter your personal email address.



6. You will receive an email via your personal email address that contains a verification code. Enter the verification code into My EPP.



7. After establishing your personal email address, you will be prompted to choose a two-step authentication option. At this point, the employee has two options to choose from for the second factor of their two-step authentication.



myEPP

Sample Page

## Two-Step Authentication

To help protect your EPP account from fraudulent activity and add extra security, we are adding two-step authentication. You can use an Authentication application or text message (SMS) as the second step. International users should use an Authentication application.

Choose an option to verify your access:

- Text Message (SMS)
- Authentication application

[Continue](#)

### What is text message (SMS)?

Each time you log into your account with your password, we'll send a one-time use code via text message (SMS) to your verified cell phone. You will then enter that code to verify your account access. Message and data rates may apply.

### What is an authentication app?

Authentication apps generate security codes for signing in to sites that require a high level of security. You can use these apps to get security codes even if you don't have an internet connection or mobile service. A mobile phone app is the typical example of an authentication app, but other forms exist, including applications for desktops, browser extensions, and physical hardware.

Any application that implements the time-based one-time password (TOTP) standard and can use a QR code or accept a manually entered key will also work.

After installing and configuring the application to work with the registrar, you will be able to receive security codes for your account. Some options for authentication apps include:

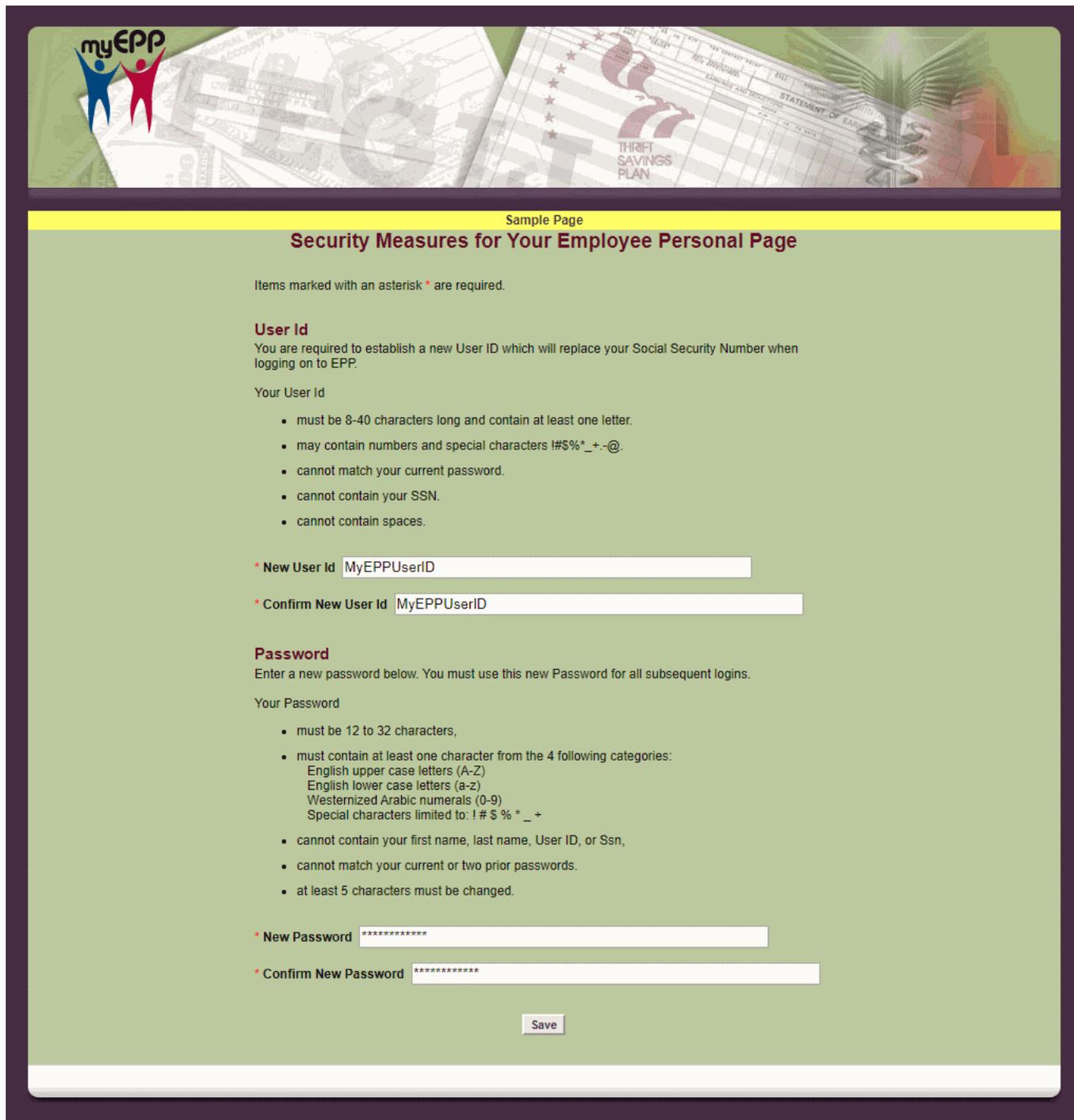
- Android: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- IOS: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- Windows: [Microsoft Authenticator](#), [1Password](#), [OneLogin OTP](#)
- Mac: [1Password](#), [OTP Manager](#)

**Please note that some authentication apps have a cost.**

 [NFC Home](#) | [Accessibility Statement](#) | [Security](#) | [Privacy Policy](#) | [Contact Us](#) | 12/19/2019 P22 1

## If you use a user ID and password to log into My EPP:

1. Enter your user ID and password and select the log in button.
2. Once logged in, you will be prompted to create a user ID and password (if you are a new user).



The image shows a sample page for setting up security measures. At the top, there is a banner with the 'myEPP' logo (two stylized figures, one blue and one red) and a background collage of financial documents, including a 'THIRTI SAVINGS PLAN' statement. Below the banner is a yellow header bar with the text 'Sample Page'. The main content area has a green background and is titled 'Security Measures for Your Employee Personal Page'. It includes instructions and requirements for creating a new User ID and Password, with asterisks indicating required fields. The form contains input boxes for 'New User Id' and 'Confirm New User Id', both containing the text 'MyEPPUserID'. Below that are input boxes for 'New Password' and 'Confirm New Password', both containing a series of asterisks. A 'Save' button is located at the bottom of the form area.

myEPP

THIRTI SAVINGS PLAN

Sample Page

### Security Measures for Your Employee Personal Page

Items marked with an asterisk \* are required.

#### User Id

You are required to establish a new User ID which will replace your Social Security Number when logging on to EPP.

Your User Id

- must be 8-40 characters long and contain at least one letter.
- may contain numbers and special characters !#\$%\*\_+.-@.
- cannot match your current password.
- cannot contain your SSN.
- cannot contain spaces.

\* New User Id

\* Confirm New User Id

#### Password

Enter a new password below. You must use this new Password for all subsequent logins.

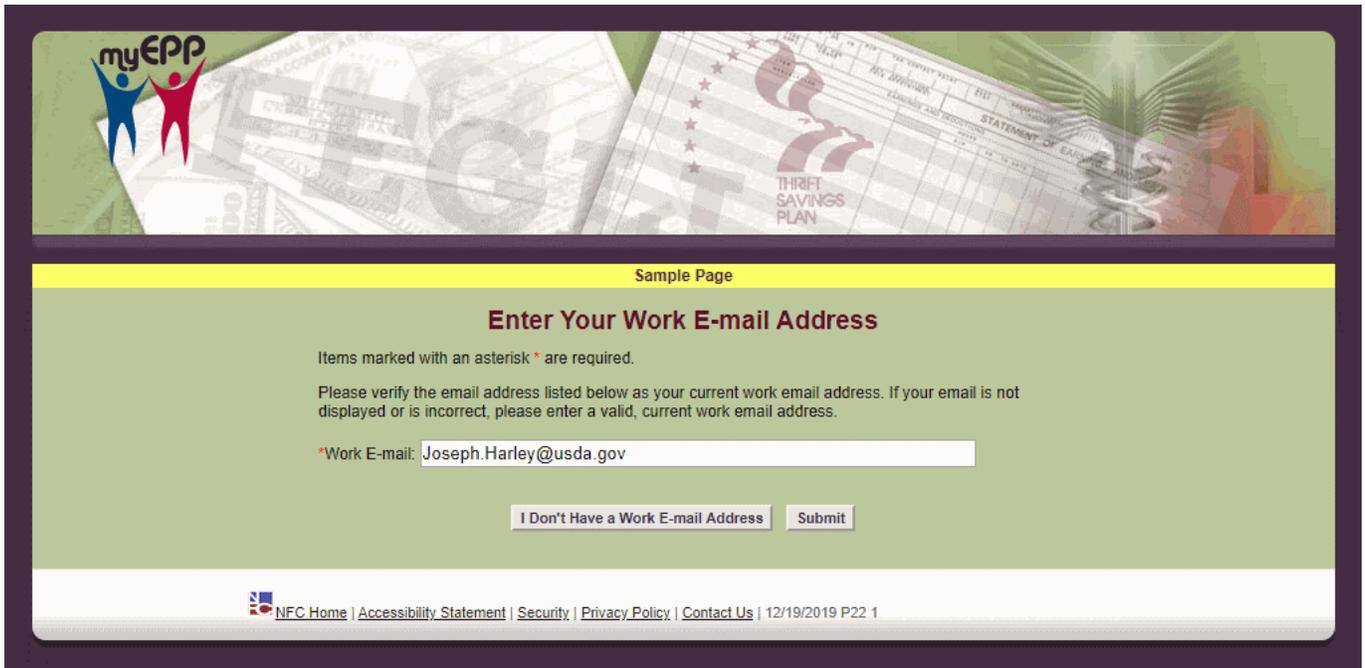
Your Password

- must be 12 to 32 characters,
- must contain at least one character from the 4 following categories:
  - English upper case letters (A-Z)
  - English lower case letters (a-z)
  - Westernized Arabic numerals (0-9)
  - Special characters limited to: ! # \$ % \* \_ +
- cannot contain your first name, last name, User ID, or Ssn,
- cannot match your current or two prior passwords.
- at least 5 characters must be changed.

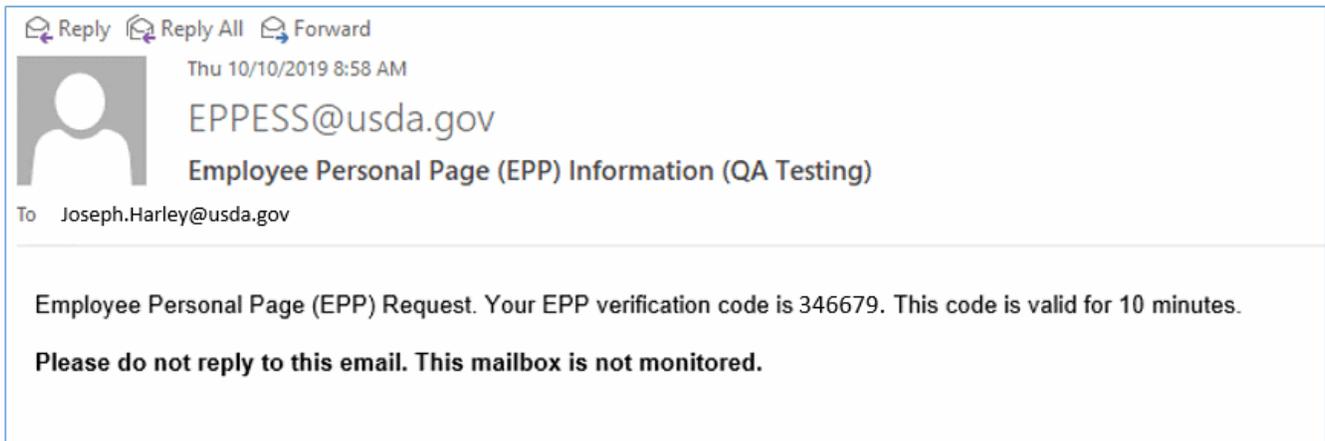
\* New Password

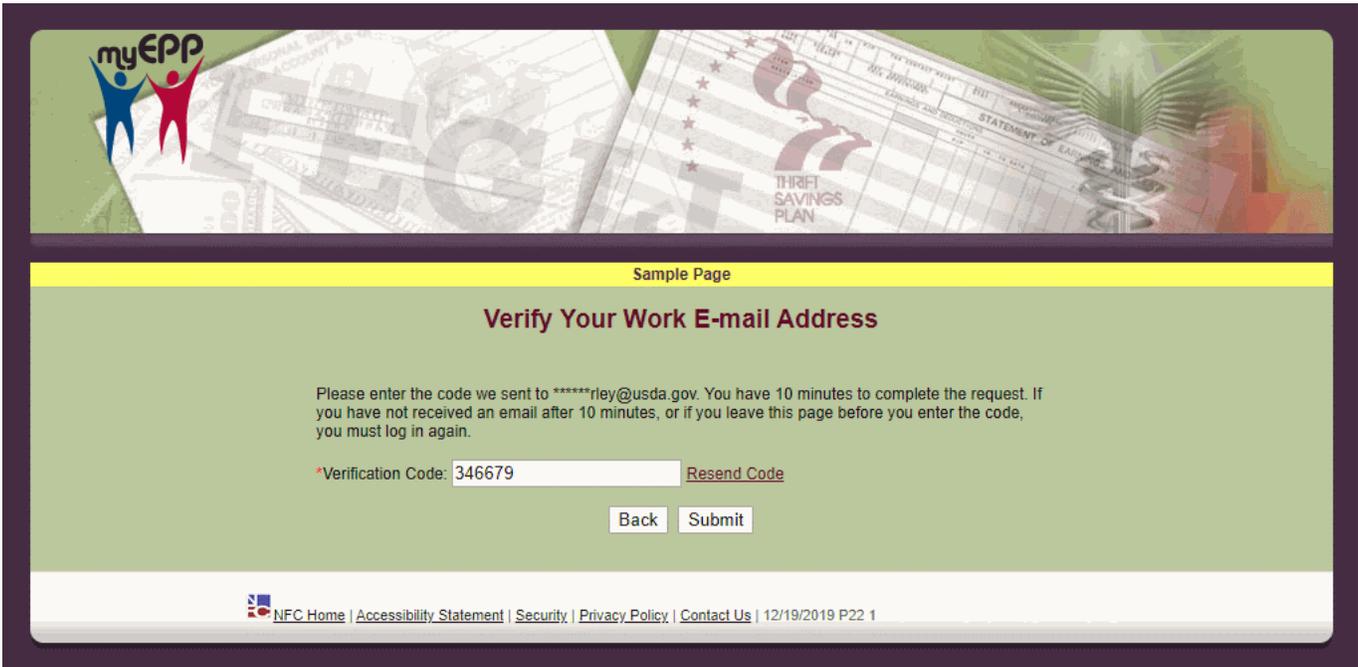
\* Confirm New Password

3. After establishing your user ID and password, you will be prompted to enter or edit your work email address. If you do not have a work email address, please select "I Don't Have a Work Email Address."

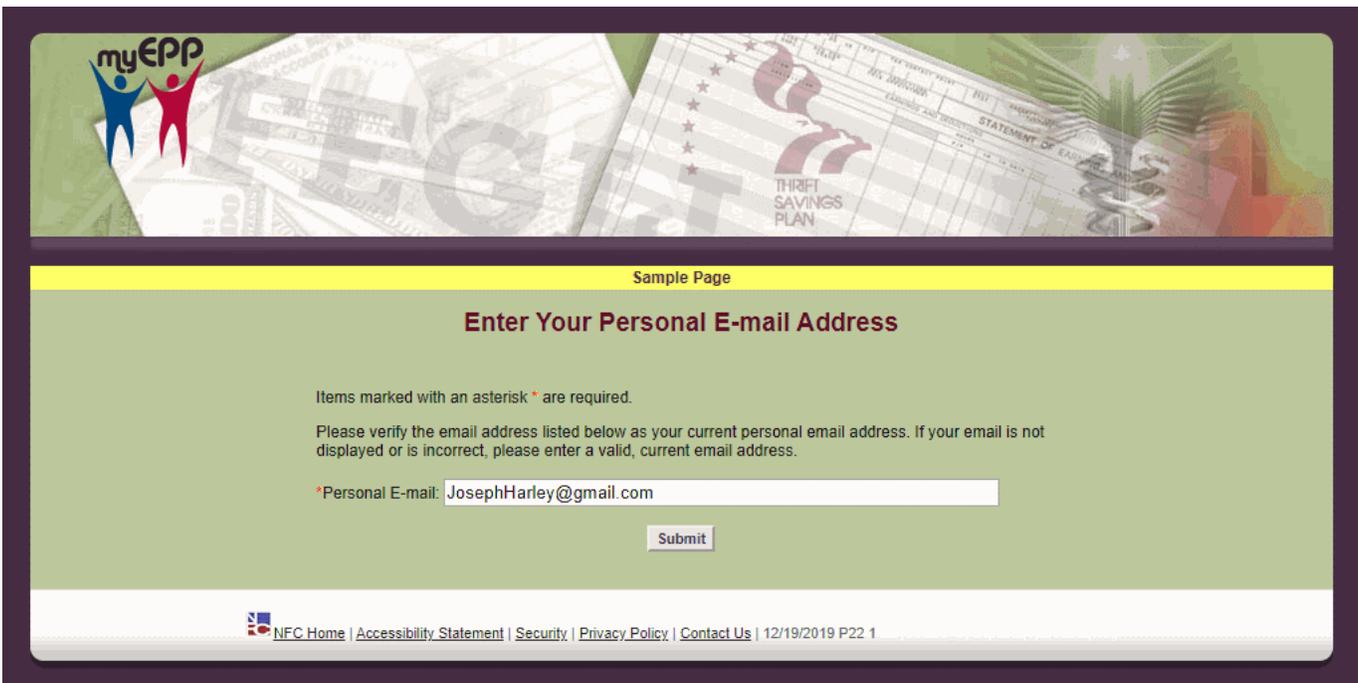


4. You will receive an email via your work email address that contains a verification code. Enter the verification code into My EPP.

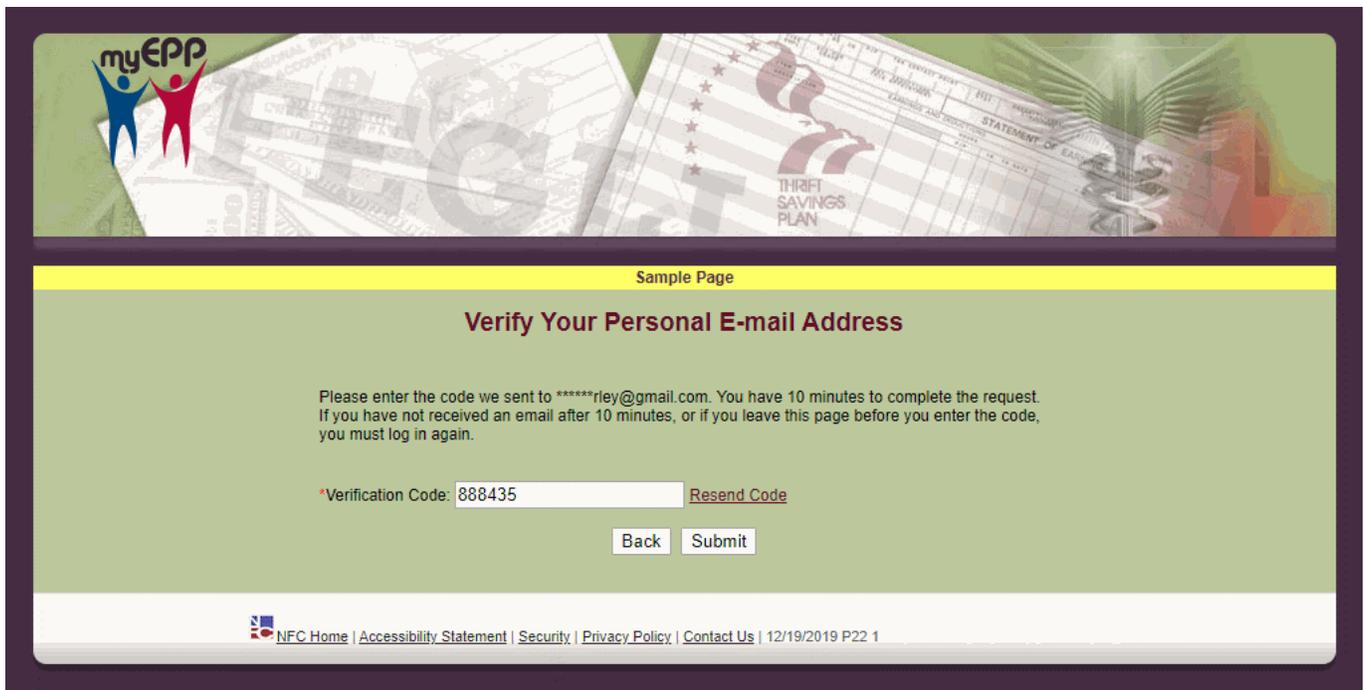
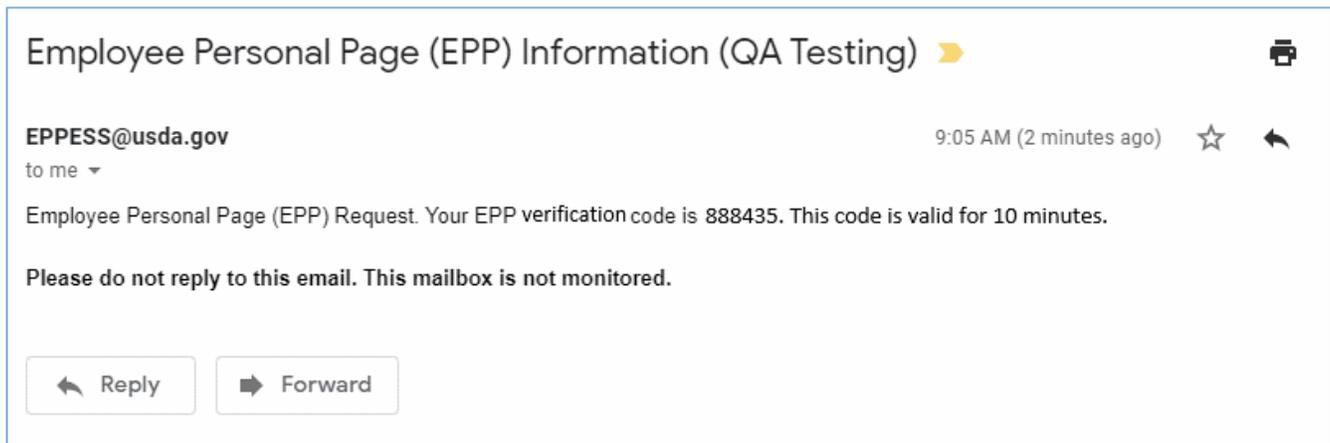




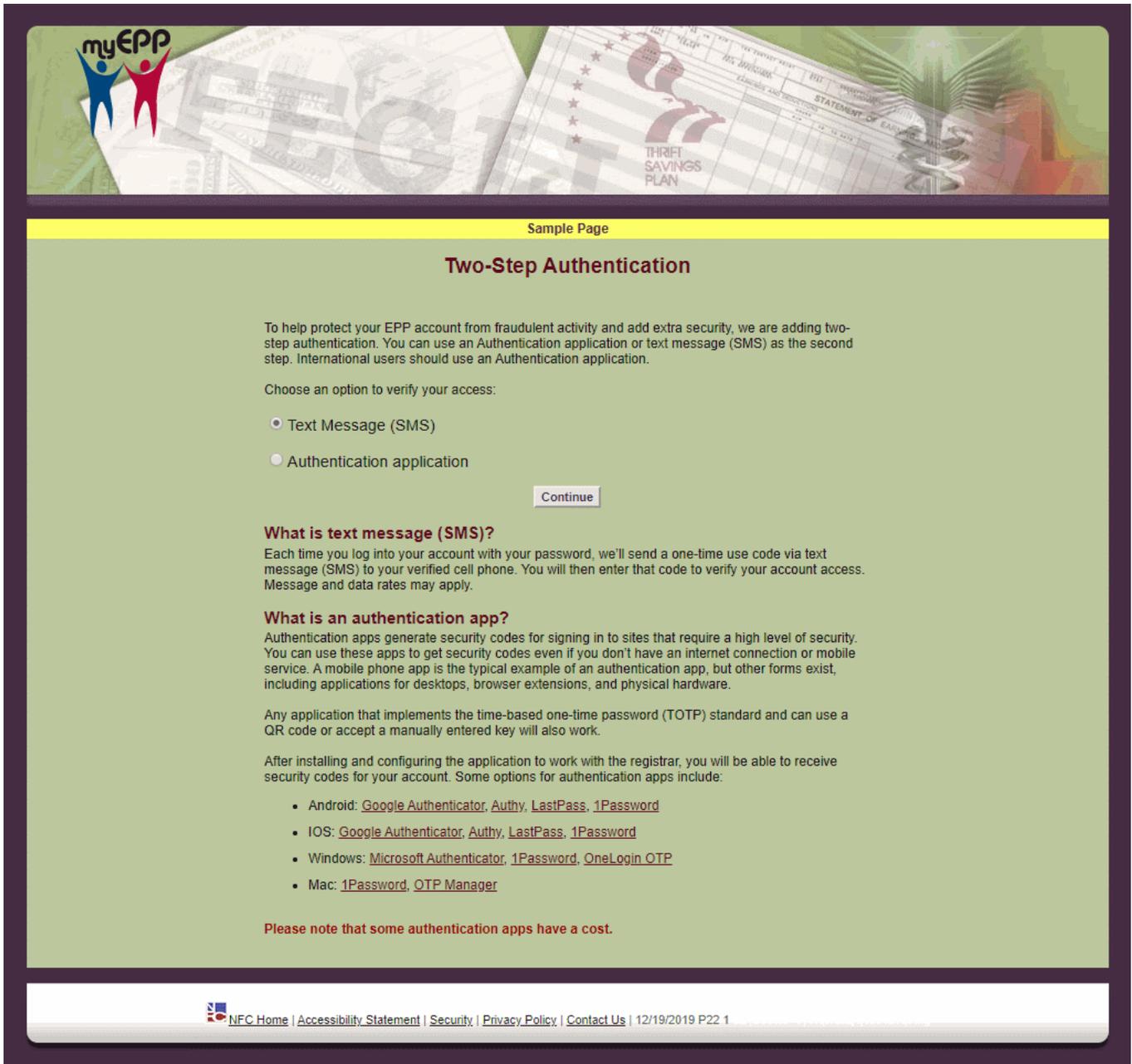
5. After verifying your work email address, you will be prompted to enter your personal email address.



6. You will receive an email via your personal email address that contains a verification code. Enter the verification code into My EPP.



7. After establishing your personal email address, you will be prompted to choose a two-step authentication option. At this point, the employee has two options to choose from for the second factor of their two-step authentication.



myEPP

Sample Page

## Two-Step Authentication

To help protect your EPP account from fraudulent activity and add extra security, we are adding two-step authentication. You can use an Authentication application or text message (SMS) as the second step. International users should use an Authentication application.

Choose an option to verify your access:

- Text Message (SMS)
- Authentication application

[Continue](#)

### What is text message (SMS)?

Each time you log into your account with your password, we'll send a one-time use code via text message (SMS) to your verified cell phone. You will then enter that code to verify your account access. Message and data rates may apply.

### What is an authentication app?

Authentication apps generate security codes for signing in to sites that require a high level of security. You can use these apps to get security codes even if you don't have an internet connection or mobile service. A mobile phone app is the typical example of an authentication app, but other forms exist, including applications for desktops, browser extensions, and physical hardware.

Any application that implements the time-based one-time password (TOTP) standard and can use a QR code or accept a manually entered key will also work.

After installing and configuring the application to work with the registrar, you will be able to receive security codes for your account. Some options for authentication apps include:

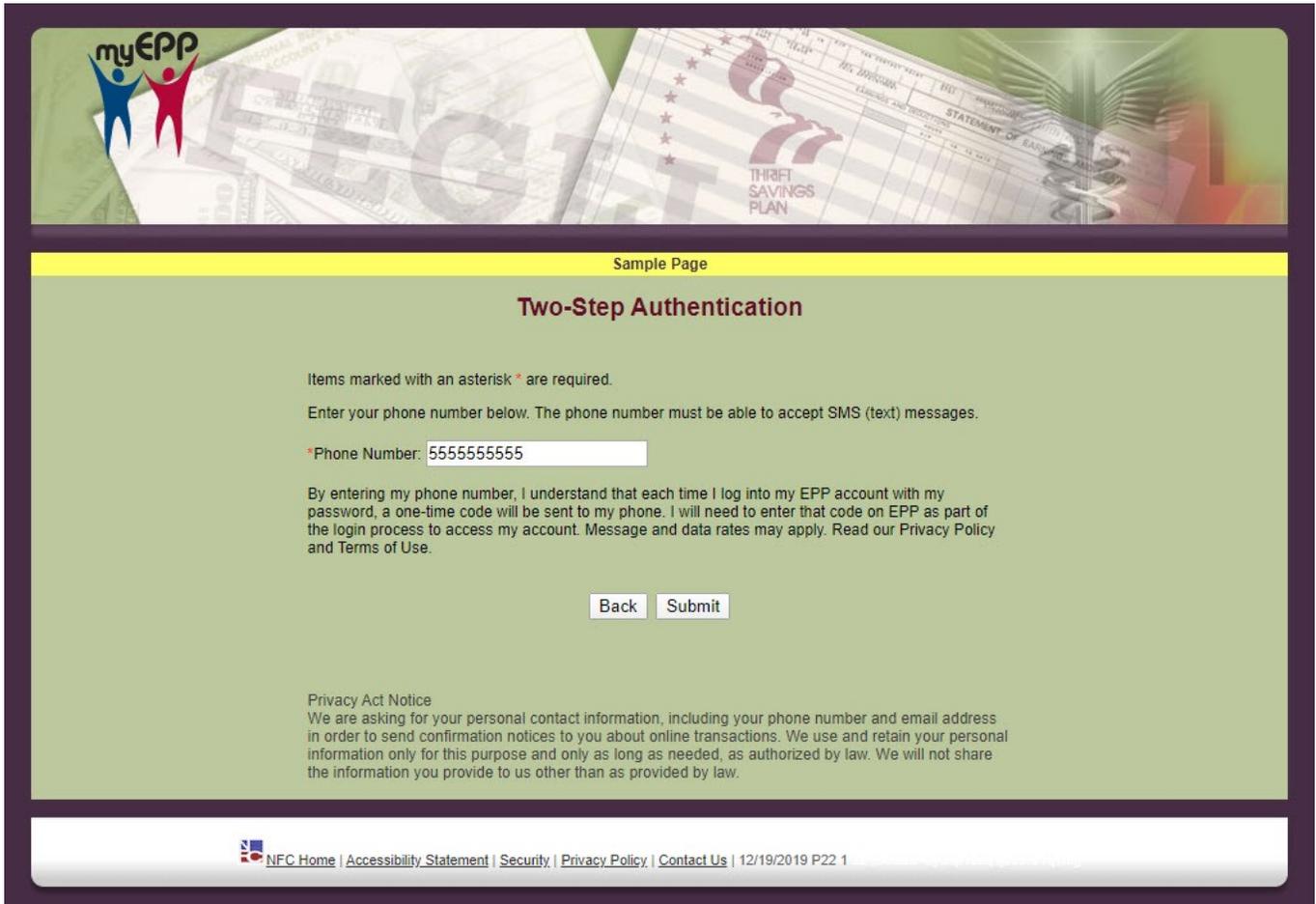
- Android: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- IOS: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- Windows: [Microsoft Authenticator](#), [1Password](#), [OneLogin OTP](#)
- Mac: [1Password](#), [OTP Manager](#)

**Please note that some authentication apps have a cost.**

 [NFC Home](#) | [Accessibility Statement](#) | [Security](#) | [Privacy Policy](#) | [Contact Us](#) | 12/19/2019 P22 1

## Text Message (SMS) Authentication Option

1. If you choose the **Text Message (SMS)** option, you will be prompted to enter your phone number and select submit.



myEPP

Sample Page

### Two-Step Authentication

Items marked with an asterisk \* are required.

Enter your phone number below. The phone number must be able to accept SMS (text) messages.

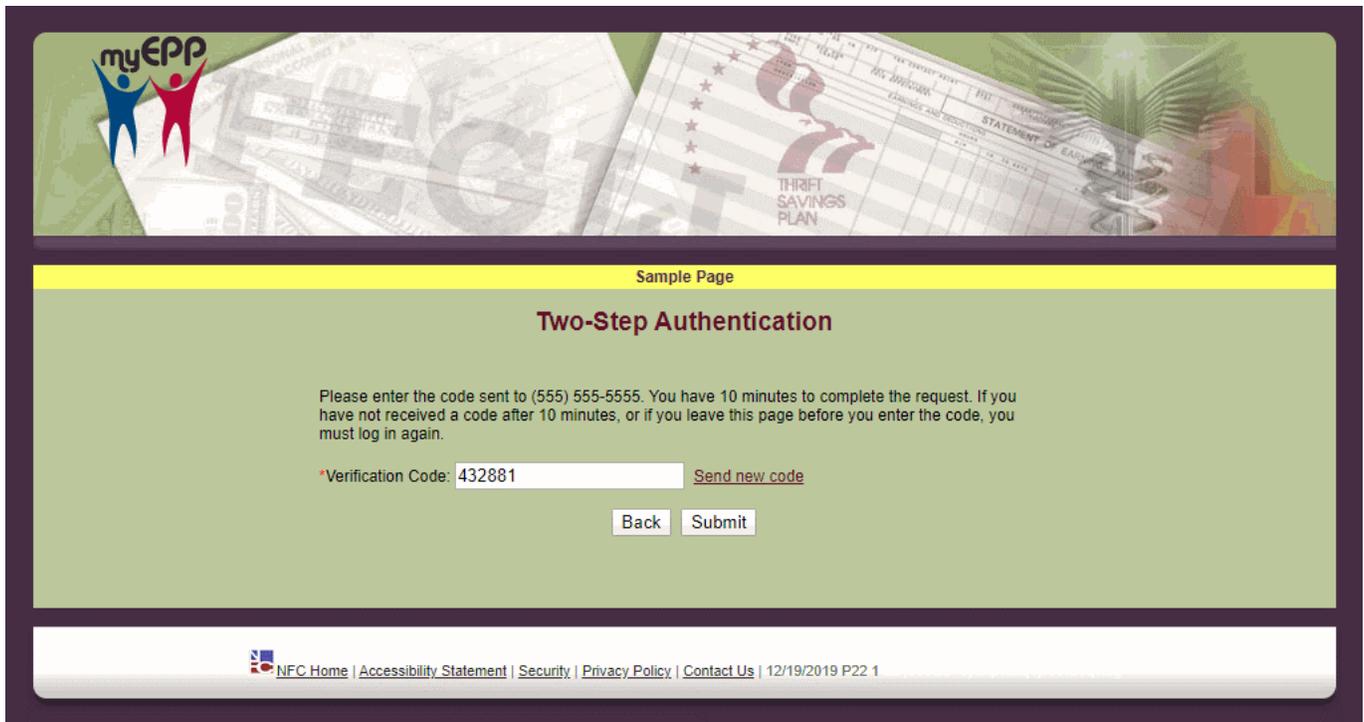
\*Phone Number:

By entering my phone number, I understand that each time I log into my EPP account with my password, a one-time code will be sent to my phone. I will need to enter that code on EPP as part of the login process to access my account. Message and data rates may apply. Read our [Privacy Policy](#) and [Terms of Use](#).

Privacy Act Notice  
We are asking for your personal contact information, including your phone number and email address in order to send confirmation notices to you about online transactions. We use and retain your personal information only for this purpose and only as long as needed, as authorized by law. We will not share the information you provide to us other than as provided by law.

 [NFC Home](#) | [Accessibility Statement](#) | [Security](#) | [Privacy Policy](#) | [Contact Us](#) | 12/19/2019 P22 1

2. You will receive a verification code via text message on your phone. Enter the verification code into My EPP.



3. After establishing your phone number, you will receive a text message confirming that two-factor authentication has been enabled for My EPP and you will then be logged into the My EPP application

## Authentication Application Option

1. If you choose **authentication application**, you will be shown a text-based verification code and a QR code.

**myEPP**

Pay Period Calendar Help Contact Us Log out

### Two-Step Authentication

To help protect your EPP account from fraudulent activity and add extra security, we are adding two-step authentication. You can use an Authentication application or text message (SMS) as the second step.

Text message (SMS) is available in the US only. If you are outside of the US, you must use the Authentication application option.

Choose an option to verify your access:

Text Message (SMS)

Authentication application

Continue

#### What is text message (SMS)?

Each time you log into your account with your password, we will send a one-time use code via text message (SMS) to your verified phone number. You will then enter that code to verify your account access. Message and data rates may apply.

#### What is an authentication app?

Authentication apps generate security codes without requiring internet connection or mobile service. You just need to download an authentication app to your computer or phone. Some options for authentication apps are:

- Android: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- IOS: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- Windows: [Google Authenticator](#), [1Password](#), [OneLogin OTP](#)
- Mac: [1Password](#), [OTP Manager](#)
- Chrome: [Authenticator](#)
- Firefox: [GAuth Authenticator](#)

v1.16.0.1 P10 2

2. You can choose to enter the text-based verification code OR scan the QR code with your phone via the app.

myEPP

Pay Period Calendar Help Contact Us Log out

### Two-Step Authentication

Get your code from an authentication app.

1. Open your authentication app
2. Enter this key in the app

or

Scan code

3. Enter the code from the app

v1.16.0.1 P10 2

3. Once you have verified through the authentication application you will then be logged into My EPP.

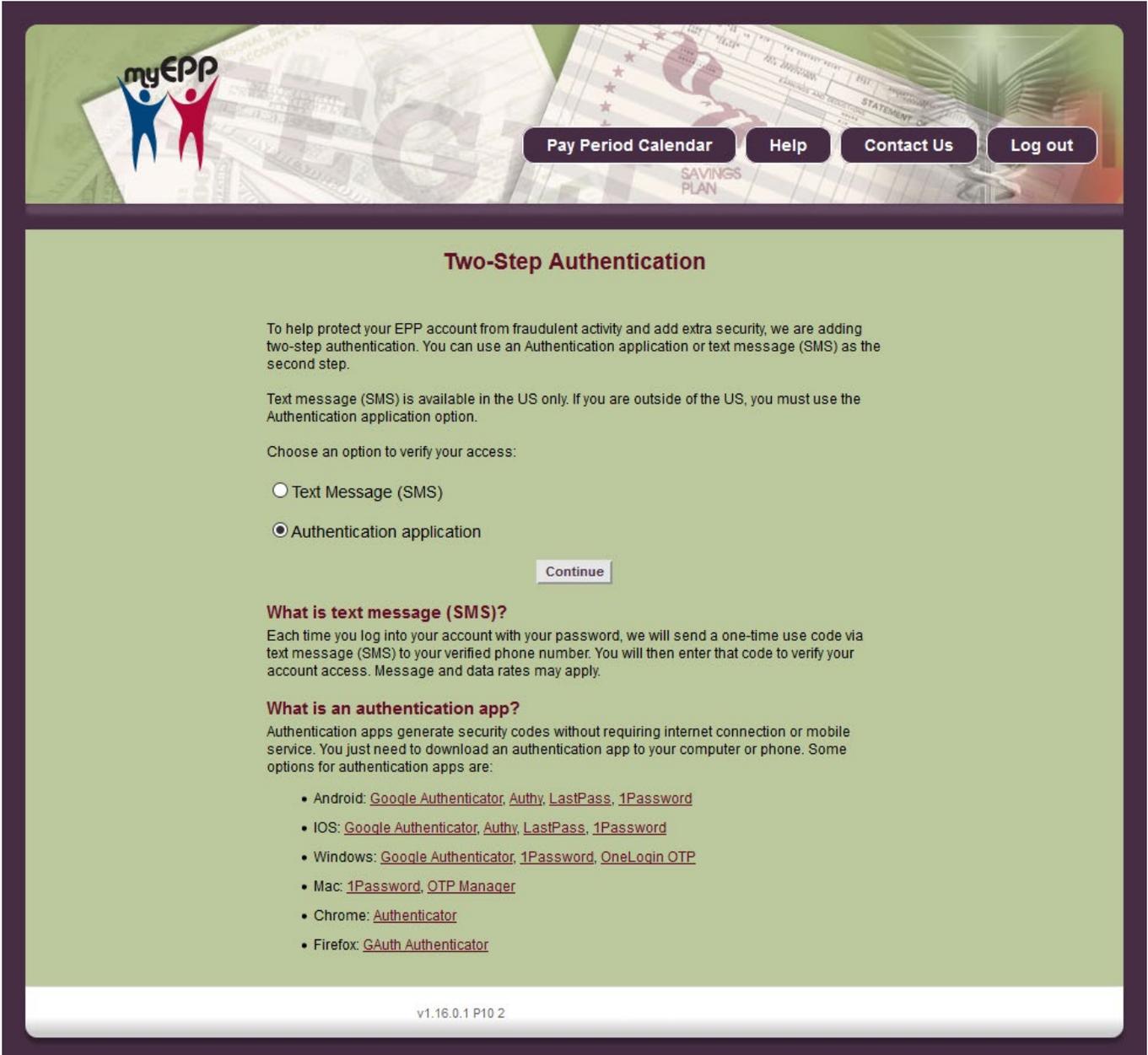
## How do I change my two-factor authentication options (phone number or email)?

1. Visit the [NFC Home page](#) and select the My EPP icon from the application launch pad.
2. View/read the warning page and select "I agree" to access the My EPP log in page.
3. Log in to My EPP with either your user ID and password or via eAuthentication.
4. Select the Preferences menu option and a drop-down menu will appear. Select the Change Two-Step Authentication menu option.
5. Select Reset Security and follow the prompts to change your old authentication settings. You will be prompted to enter the verification code sent to your "verified" work email address (this is the work email address that was verified when you logged in and set up two-step authentication), your personal email address, or the telephone number associated with your two-step authentication.
6. You will be prompted to choose a new two-step authentication option. The prompts will then follow the same process as the first-time setup.

## What if I do not have the use of SMS text message?

As an alternative method to receiving a verification code via SMS text messaging, you may also utilize an authentication application.

- NFC provides a list of possible authentication applications for employees to use on the two-factor authentication screen in My EPP, but they may use other authentication applications or browser plugins. Authentication applications are device specific i.e. Windows, iOS (Apple), and Android.



**myEPP**

Pay Period Calendar Help Contact Us Log out

### Two-Step Authentication

To help protect your EPP account from fraudulent activity and add extra security, we are adding two-step authentication. You can use an Authentication application or text message (SMS) as the second step.

Text message (SMS) is available in the US only. If you are outside of the US, you must use the Authentication application option.

Choose an option to verify your access:

Text Message (SMS)

Authentication application

Continue

#### What is text message (SMS)?

Each time you log into your account with your password, we will send a one-time use code via text message (SMS) to your verified phone number. You will then enter that code to verify your account access. Message and data rates may apply.

#### What is an authentication app?

Authentication apps generate security codes without requiring internet connection or mobile service. You just need to download an authentication app to your computer or phone. Some options for authentication apps are:

- Android: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- IOS: [Google Authenticator](#), [Authy](#), [LastPass](#), [1Password](#)
- Windows: [Google Authenticator](#), [1Password](#), [OneLogin OTP](#)
- Mac: [1Password](#), [OTP Manager](#)
- Chrome: [Authenticator](#)
- Firefox: [GAuth Authenticator](#)

v1.16.0.1 P10 2

- If employees are currently limited as to which applications or browser plugins they may install on their government furnished equipment they may utilize personal computers or smartphones to install the available authentication applications.

Note: Please be aware of the following in regards to using any authentication application:

- The NFC Contact Center (NCC) is not able to provide support for any authentication applications outside of what is provided via the EPP two factor setup information.
- Employees located outside of the United States cannot utilize SMS via international phone numbers to perform two factor authentication and should be directed to use an authentication application.

### **I can get an SMS text message, but I am still having problems.**

- NCC can confirm the phone number currently setup for two factor by a given employee.
- With direction from an authorized Agency point of contact, NCC can reset the two factor SMS setup to allow an employee to set a new phone number for SMS authentication.
- Employees not receiving an SMS should contact their cell provider to confirm the SMS is not being blocked from delivery. NFC has received a number of reports of T-Mobile customers and small cell carrier customers not receiving SMS until contacting their carrier technical support for assistance.
- Please allow time to receive the authentication code via SMS before requesting a second code. Some issues have been identified due to users requesting multiple codes and not using the latest code provided.

### **Is there an alternate way to authenticate via e-Auth?**

Yes, NCC can set employees to eAuthentication only if the employee works for USDA, DoJ, or DHS; upon direction of an authorized Agency point of contact.

### **I established two-factor authentication and don't remember what information I used. Can you reset it for me?**

Yes. NCC can reset the entire two-factor setup of a given employee with direction from an authorized Agency point of contact only.

## **Why is NFC not allowing the use of email for the second factor authentication?**

The Office of the Chief Information Officer (OCIO) has mandated that the two-factor authentication process is in accordance with NIST standards as a means of strengthening NFC's security posture. OCIO set forth guidelines for implementation and the use of email was restricted.

## **If an employee is unable to navigate the two-factor authentication process, how can they obtain their information from My EPP?**

The employee must contact their HR Office.

## **How do I contact NCC for assistance?**

You may contact NCC for assistance at 1-855-NFC4GOV (1-855-632-4468), from the hours of 6:30 AM to 5:00 PM Central Time, Monday through Friday (except for Federal holidays). Please be advised that you may experience extended hold times.