U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

Multifactor Authentication (MFA) Guide

December 2022

Multifactor Authentication Guide

Multifactor Authentication (MFA)

What is MFA?

Multifactor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify user's identity for a login.

Multifactor Authentication only affects external users. All users must register to use this site. Registered external users will:

- Be prompted by the system to select their preferred method to receive an MFA passcode. Users will have two options for receipt: text or soft token, such as Google Authenticator. Users will be prompted to verify their default mode of MFA passcode receipt by confirming receipt and entering a security code.
- In addition to the normal login process, enter the MFA passcode every time they log into the system. A new MFA passcode is required whenever logging into a system.

Helpful Tips Regarding MFA:

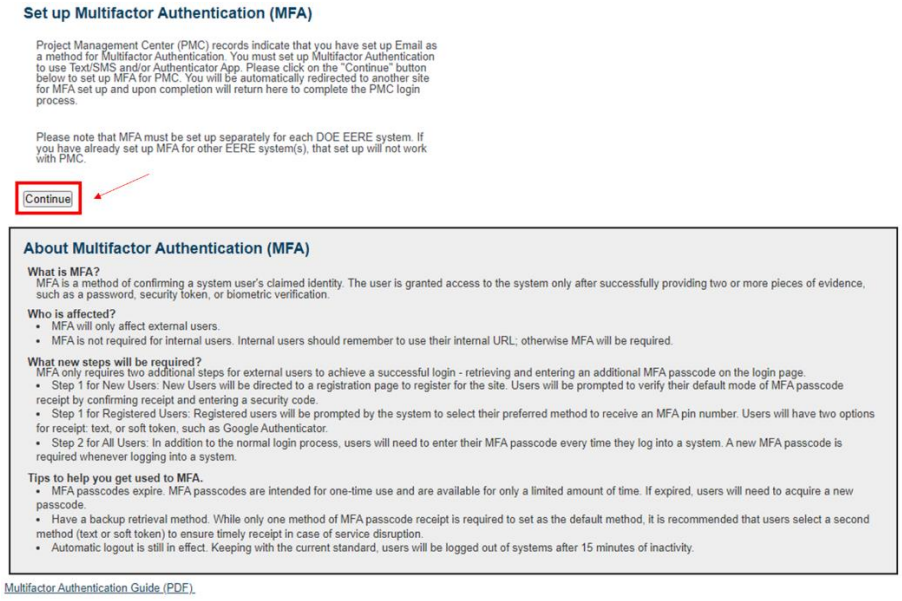
- MFA passcodes expire. MFA passcodes are intended for one-time use and are available for only a limited amount of time. If expired, users will need to acquire a new passcode.
- Have a backup retrieval method. While only one method of MFA passcode receipt is required to set as the default method, it is recommended that users select a second method (text or soft token) to ensure timely receipt in case of service disruption. You will be able to choose which of the methods to use as your default.
- Automatic logout is still in effect. Keeping with the current standard, users will be logged out of systems after 15 minutes of inactivity.

Contact ITSIHelp@ee.doe.gov with any questions

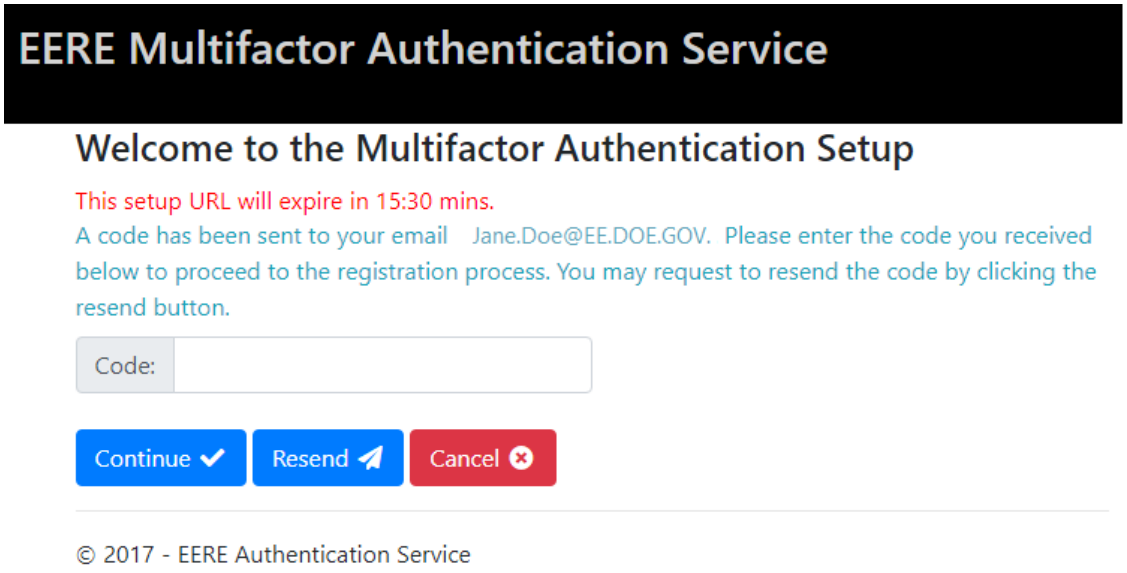
How to setup Multifactor Authentication (MFA)

1. Upon entering the site you will be asked to login normally with email and password.

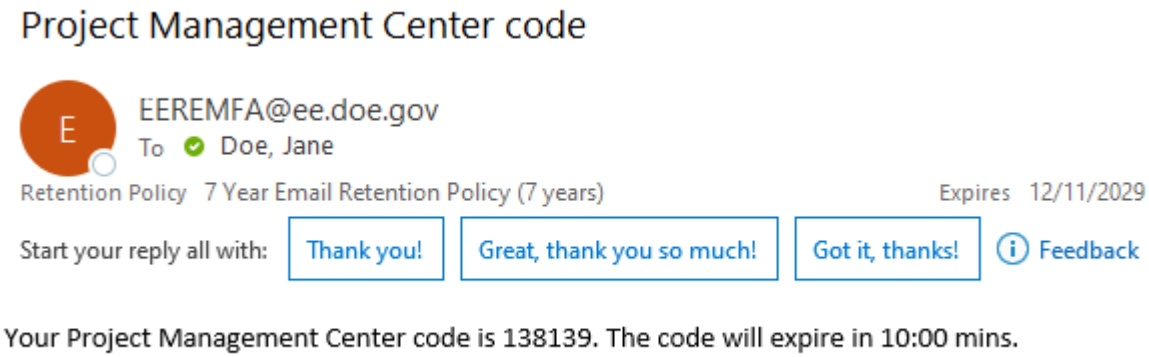
2. The Set up Multifactor Authentication (MFA) explanation screen will appear, read and click **Continue**.



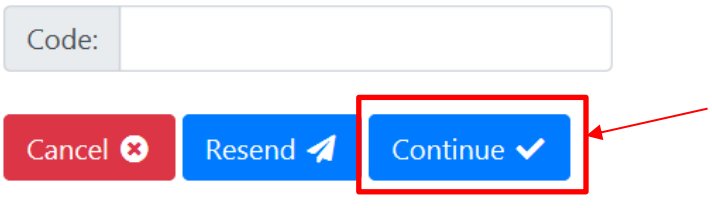
3. After you click **Continue** the MFA setup URL screen will appear. The setup process will need to be completed within the expiration time. Your email by default will be your first level of authentication, the MFA setup code will be sent to your email to proceed with the registration process.



4. The setup code will come from the EEREMFA@ee.doe.gov email address and will expire within 10 minutes.

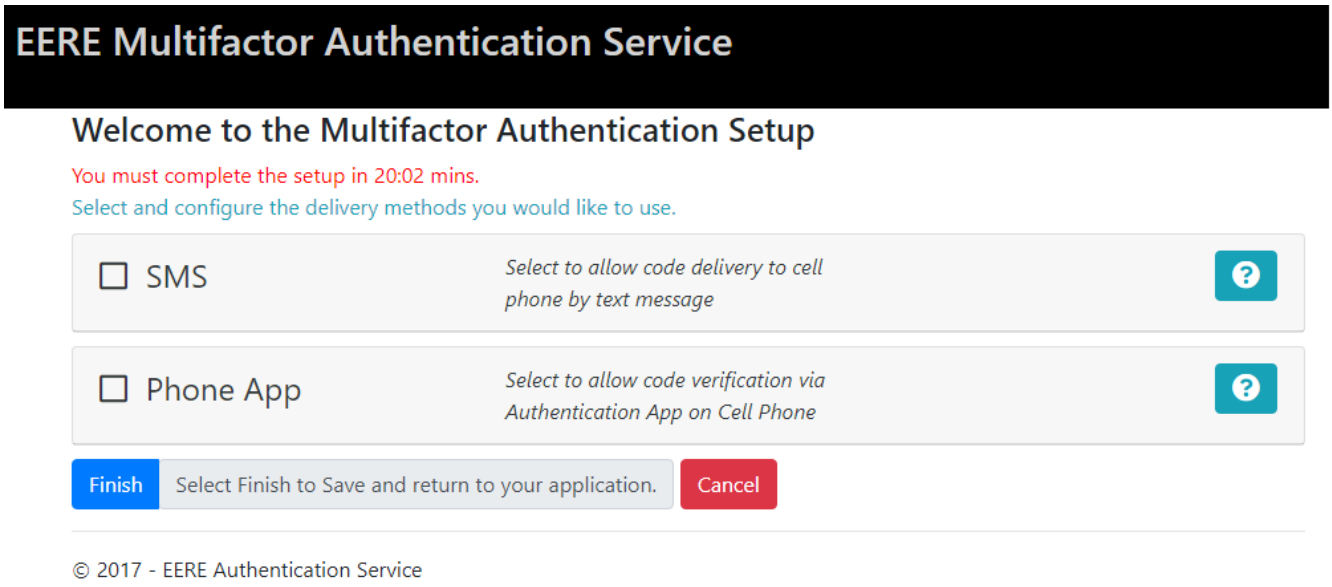


5. After you have entered the code click **Continue**.

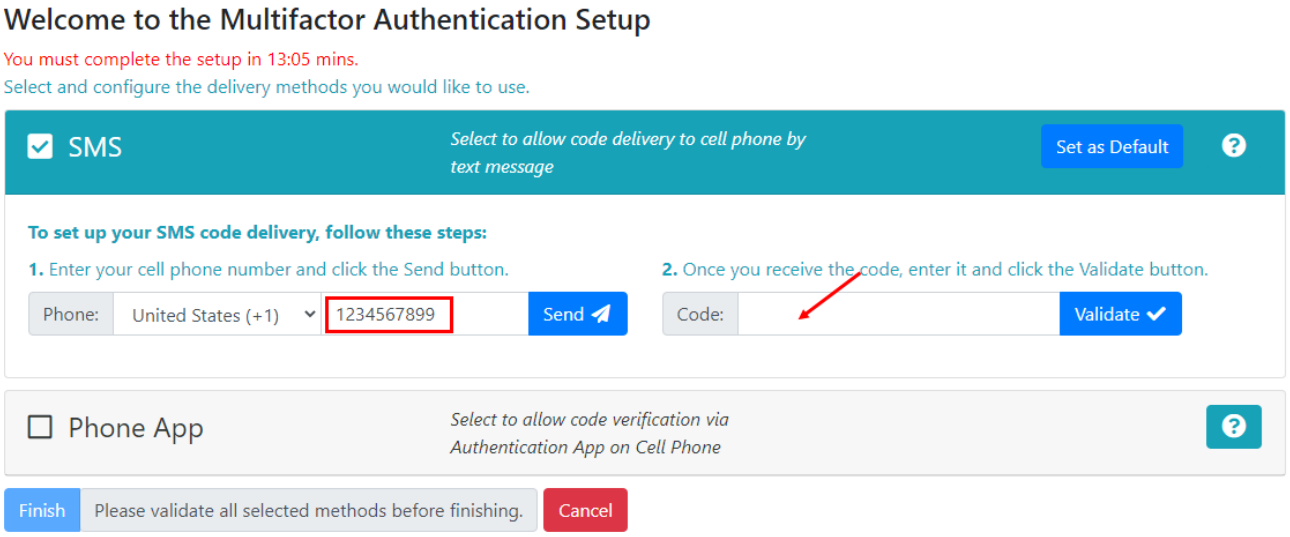


6. The **Welcome to the Multifactor Authentication Setup** screen will appear. Users will have a little over 15 minutes to complete the setup process. Two methods will be available: **SMS/ Text** delivery method and the

Authentication **Phone App** verification method.

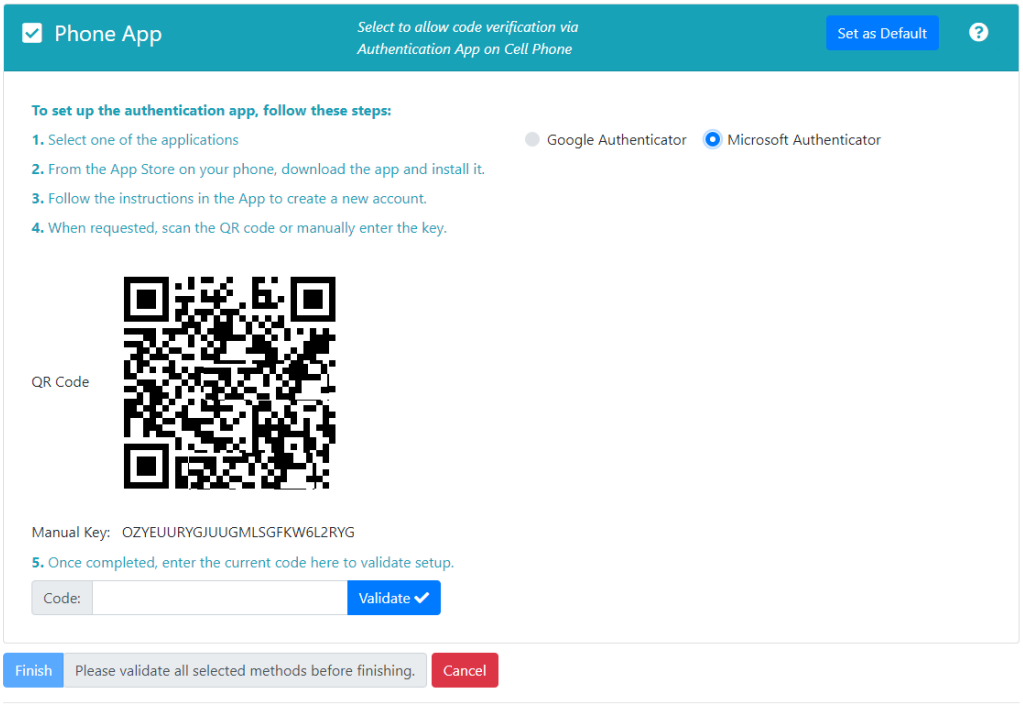


7. Choosing the **SMS delivery method** allows the authentication code to be delivered via text message to your cell phone. Enter your cell phone number, click the **Send** button and within a minute you will receive a code via text message. Enter the Code received and click the **Validate** button.



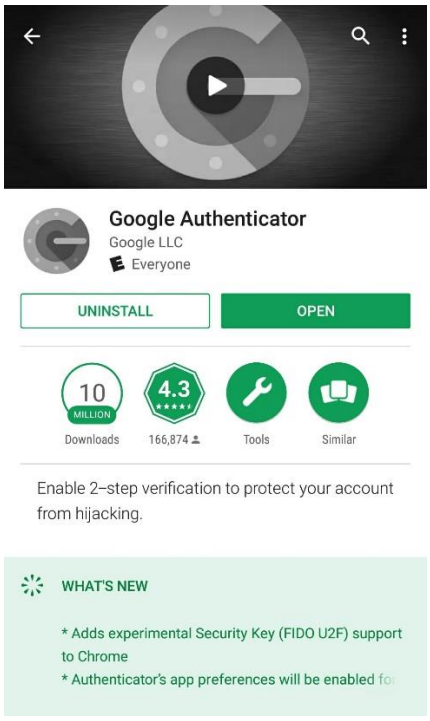
8. Once the code is validated your **SMS** delivery method will be verified 

9. The next method is the **Phone App** Authentication method. When choosing this method users will need to download either the "**Google Authenticator**" or "**Microsoft Authenticator**" apps from the app store.

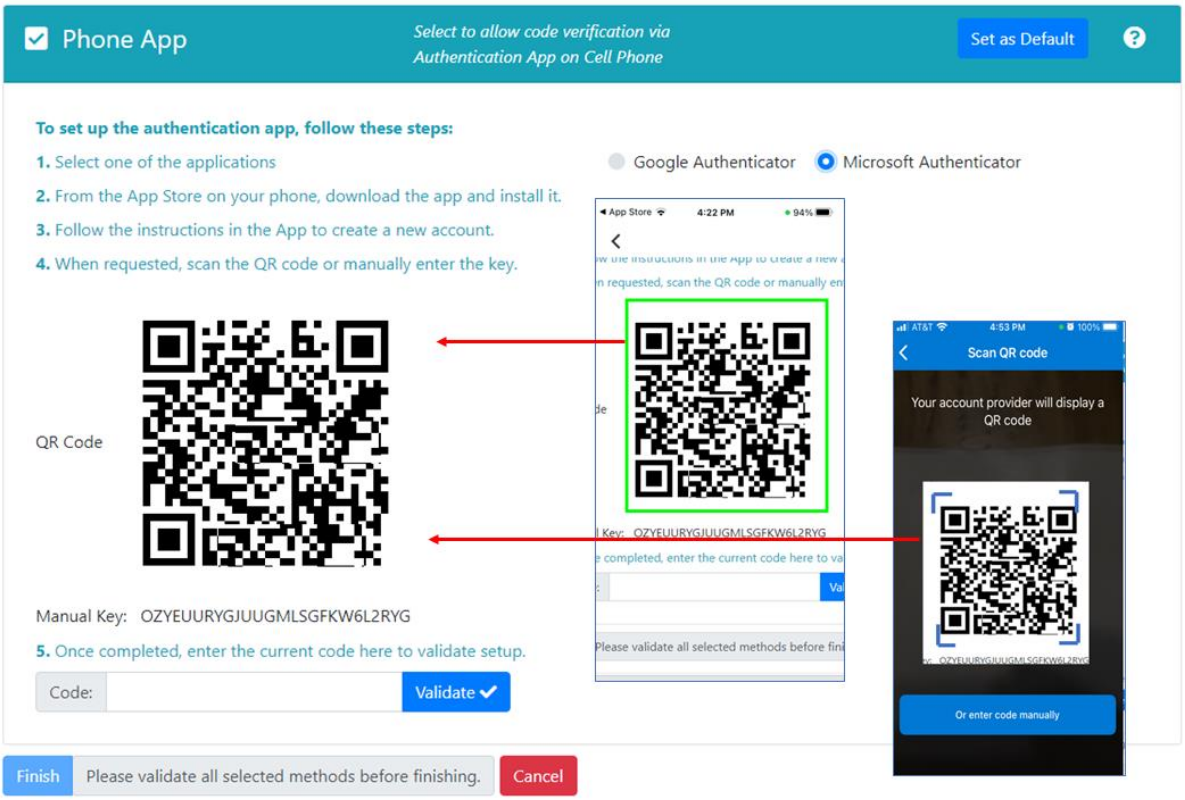


10. Once you have located and installed either app

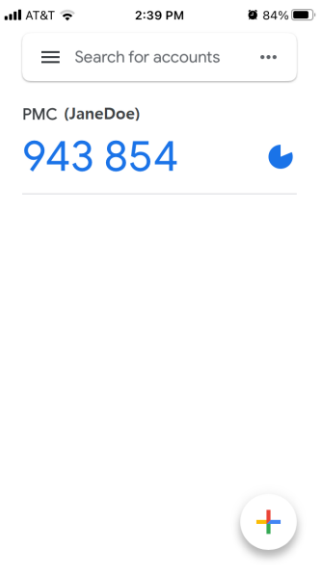
Google Authenticator or ***Microsoft Authenticator***



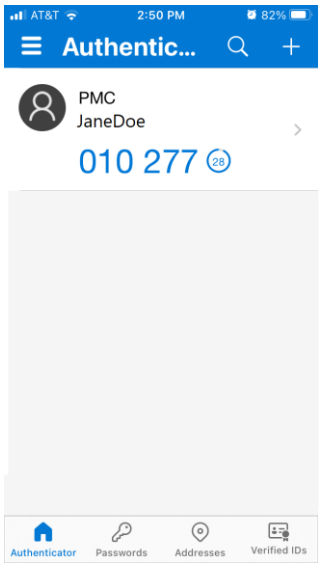
11. Either app will have a QR code scanner that Users will use to scan the **QR code** under the **Phone App** section on the screen.



12. Once the **QR Code** is scanned from your cell phone (**Google or Microsoft**) Authenticator app a code will be generated.

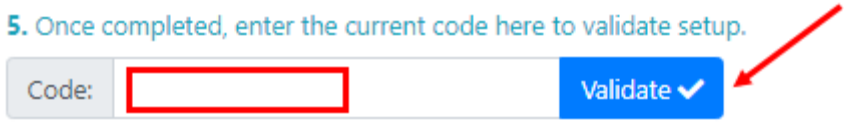


Google Authenticator



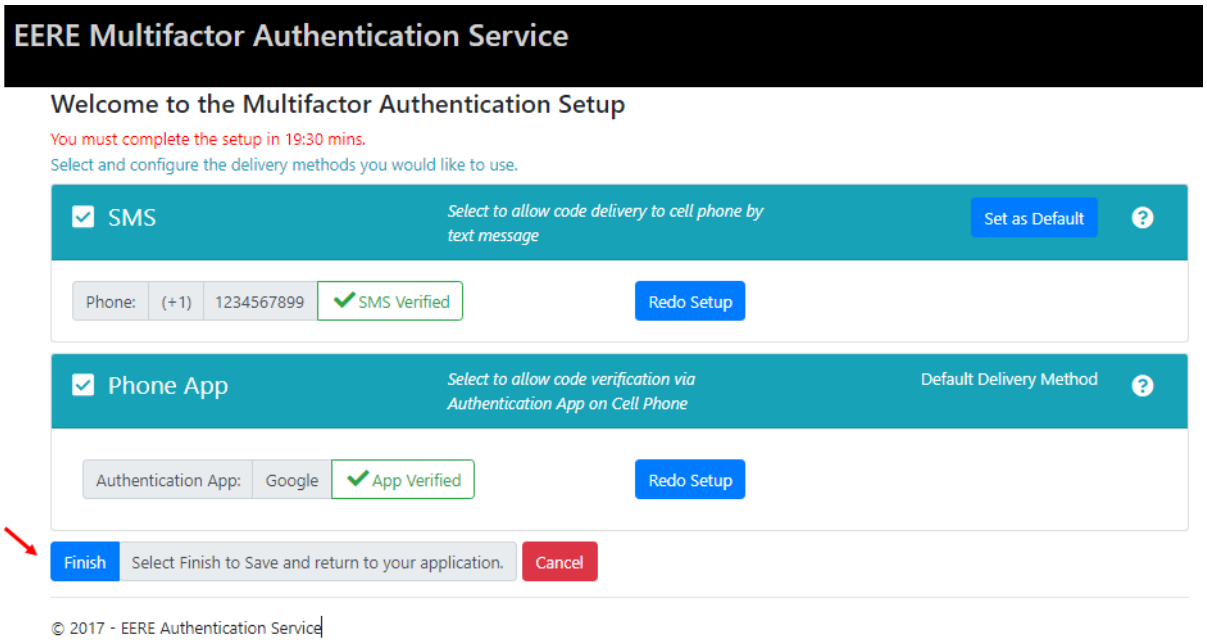
Microsoft Authenticator

13. Take this code and enter it into the **Phone App's** code area and click the **Validate** button.



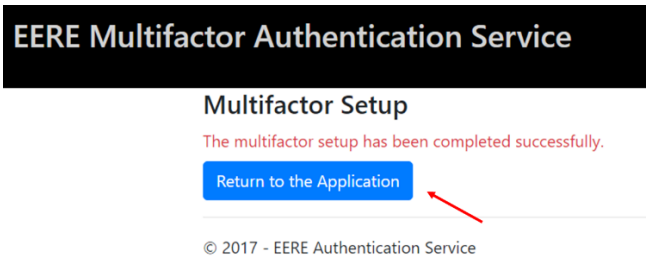
14. Once the code is validated the Phone App authentication method will be verified.

15. Once **SMS**, **Phone App**, or both are verified click the **Finish** button.

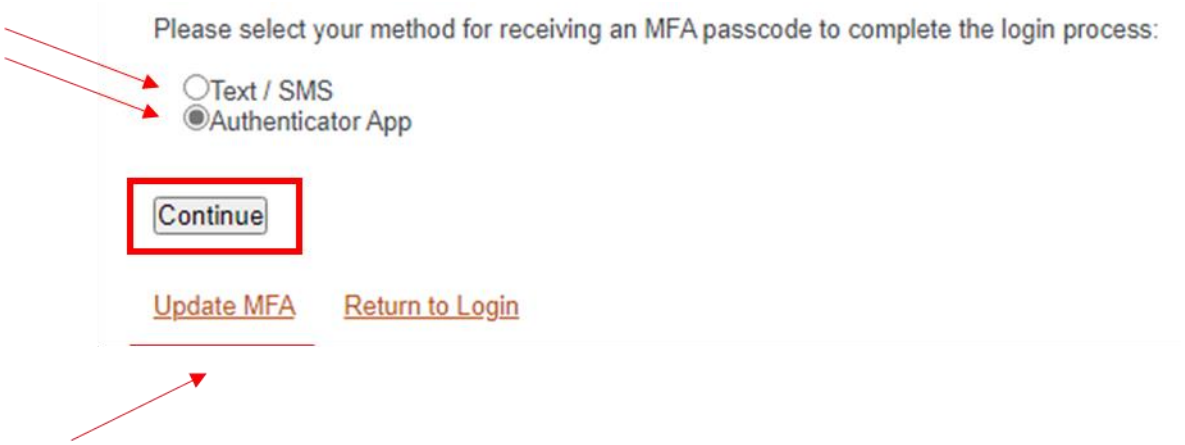


Note: It is suggested to verify both methods, that way if Users do not have access to cell phone service, then Users can still use the Phone App method without having access to their cell phone service. The Phone App verification does not require service.

16. Once the **Finish** button has been clicked the **Multifactor Setup** will be complete. Click the **Return to the Application** button.



17. Returning to the application will now give Users the option to choose the **MFA passcode** verification method of their choice (Text message or via Authenticator App) at each sign-in into the system.



*Note: At any time a User needs to redo/ update their MFA they can do so by simply clicking **Update MFA** to redo the previous setup instructions.*