



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.

Email:
Password:

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

Set up Multifactor Authentication (MFA)

Project Management Center (PMC) records indicate that you have set up Email as a method for Multifactor Authentication. You must set up Multifactor Authentication to use Text/SMS and/or Authenticator App. Please click on the "Continue" button below to set up MFA for PMC. You will be automatically redirected to another site for MFA set up and upon completion will return here to complete the PMC login process.

Please note that MFA must be set up separately for each DOE EERE system. If you have already set up MFA for other EERE system(s), that set up will not work with PMC.

About Multifactor Authentication (MFA)

What is MFA?
MFA is a method of confirming a system user's claimed identity. The user is granted access to the system only after successfully providing two or more pieces of evidence, such as a password, security token, or biometric verification.

Who is affected?

- MFA will only affect external users.
- MFA is not required for internal users. Internal users should remember to use their internal URL; otherwise MFA will be required.

What new steps will be required?
MFA only requires two additional steps for external users to achieve a successful login - retrieving and entering an additional MFA passcode on the login page.

- Step 1 for New Users: New Users will be directed to a registration page to register for the site. Users will be prompted to verify their default mode of MFA passcode receipt by confirming receipt and entering a security code.
- Step 1 for Registered Users: Registered users will be prompted by the system to select their preferred method to receive an MFA pin number. Users will have two options for receipt: text, or soft token, such as Google Authenticator.
- Step 2 for All Users: In addition to the normal login process, users will need to enter their MFA passcode every time they log into a system. A new MFA passcode is required whenever logging into a system.

Tips to help you get used to 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.
- Automatic logout is still in effect. Keeping with the current standard, users will be logged out of systems after 15 minutes of inactivity.

[Multifactor Authentication Guide \(PDF\)](#)

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.

EERE Multifactor Authentication Service

Welcome to the Multifactor Authentication Setup

This setup URL will expire in 15:30 mins.

A code has been sent to your email Jane.Doe@EE.DOE.GOV. Please enter the code you received below to proceed to the registration process. You may request to resend the code by clicking the resend button.

Code:

[Continue ✓](#) [Resend ↗](#) [Cancel ✕](#)

© 2017 - EERE Authentication Service

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

Project Management Center code

 EEREMFA@ee.doe.gov
To  Doe, Jane

Retention Policy 7 Year Email Retention Policy (7 years) Expires 12/11/2029

Start your reply all with: [Thank you!](#) [Great, thank you so much!](#) [Got it, thanks!](#) [Feedback](#)

Your Project Management Center code is 138139. The code will expire in 10:00 mins.

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

Code:

[Cancel ✕](#) [Resend ↗](#) [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.

EERE Multifactor Authentication Service

Welcome to the Multifactor Authentication Setup

You must complete the setup in 20:02 mins.

Select and configure the delivery methods you would like to use.

<input type="checkbox"/> SMS	Select to allow code delivery to cell phone by text message	
<input type="checkbox"/> Phone App	Select to allow code verification via Authentication App on Cell Phone	
Finish	Select Finish to Save and return to your application.	Cancel

© 2017 - EERE Authentication Service

- 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.

Welcome to the Multifactor Authentication Setup

You must complete the setup in 13:05 mins.

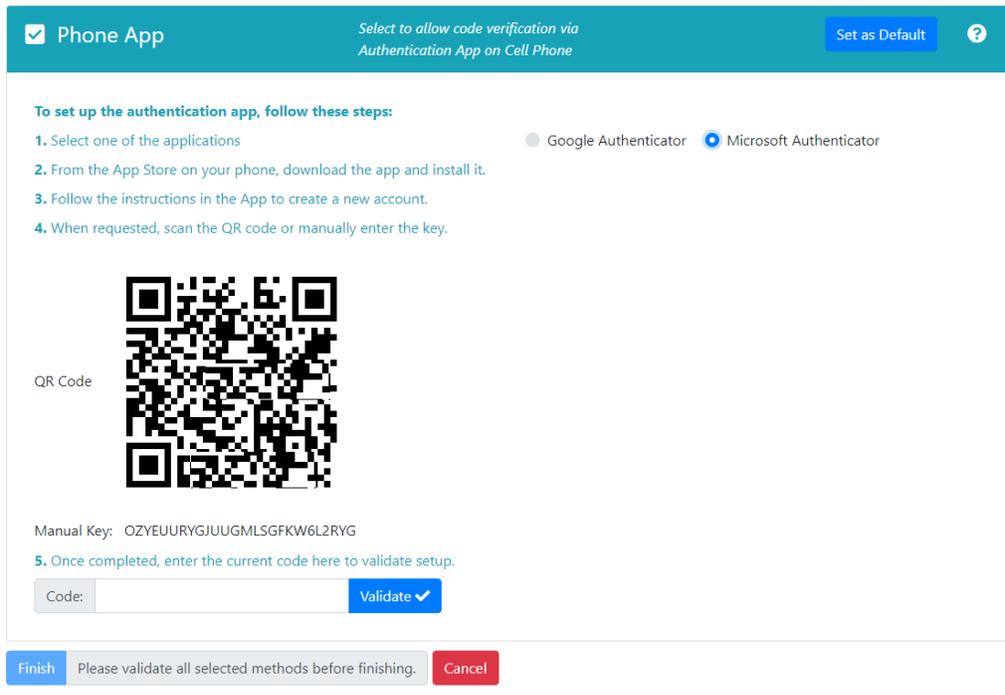
Select and configure the delivery methods you would like to use.

<input checked="" type="checkbox"/> SMS	Select to allow code delivery to cell phone by text message	Set as Default	
To set up your SMS code delivery, follow these steps:			
1. Enter your cell phone number and click the Send button.		2. Once you receive the code, enter it and click the Validate button.	
Phone:	United States (+1) <input type="text" value="1234567899"/>	Send	Code: <input type="text"/> Validate
<input type="checkbox"/> Phone App	Select to allow code verification via Authentication App on Cell Phone		
Finish	Please validate all selected methods before finishing.	Cancel	

- 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.



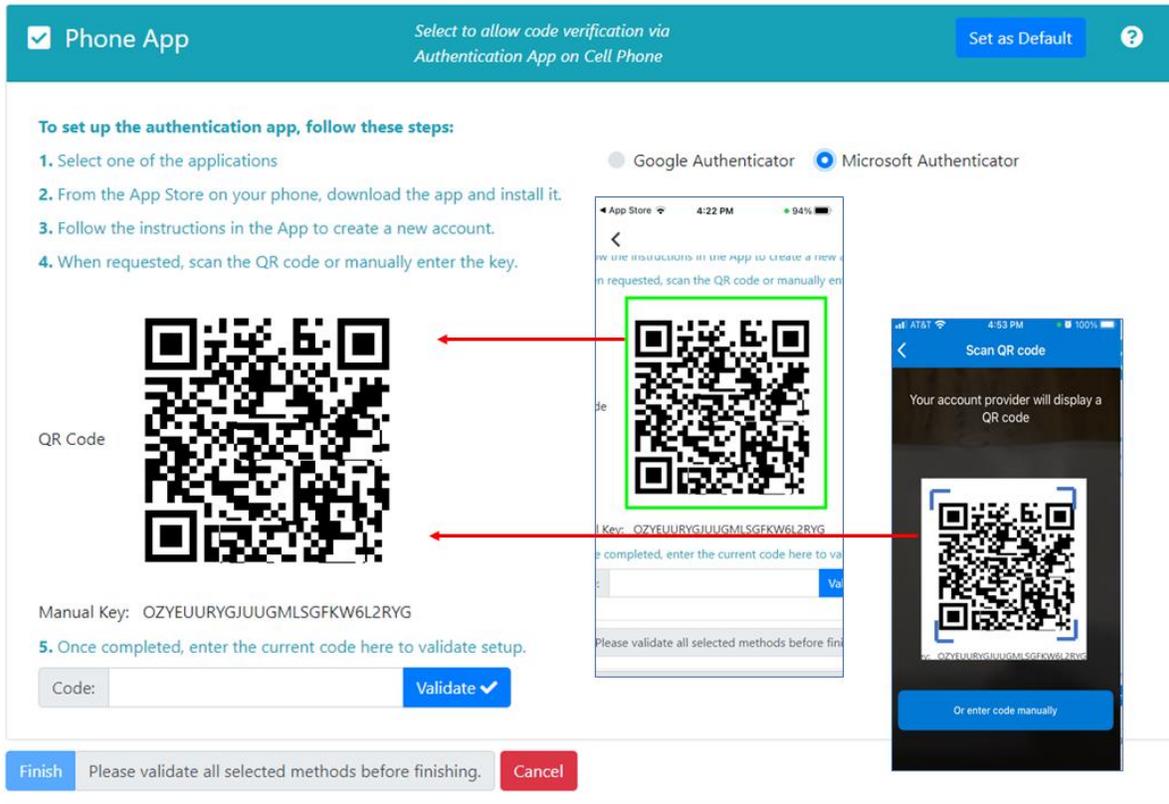
10. Once you have located and installed either app



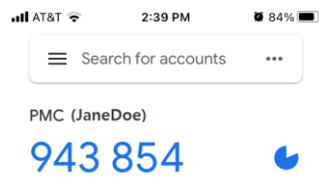
or



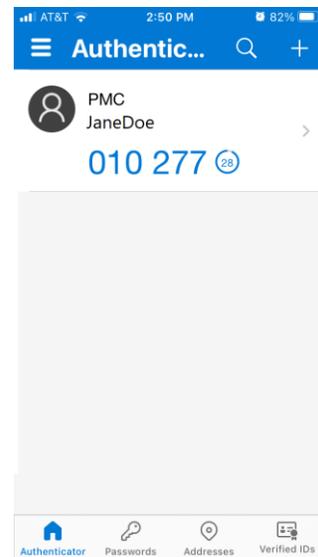
11. Either app will have a QR code scanner that Users will use to scan the **QR code** under the **Phone App** section on the screen.



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.

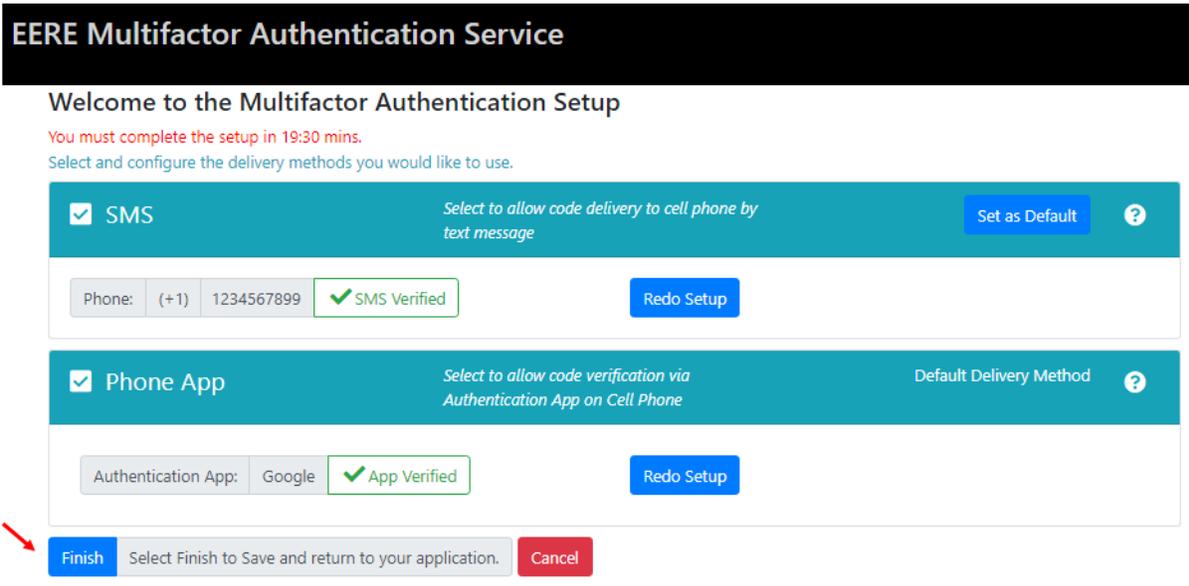
5. Once completed, enter the current code here to validate setup.

A form element for code validation. It consists of a grey label 'Code:' followed by a white input field with a red border. To the right of the input field is a blue button with the text 'Validate' and a white checkmark icon. A red arrow points from the top right towards the 'Validate' button.

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

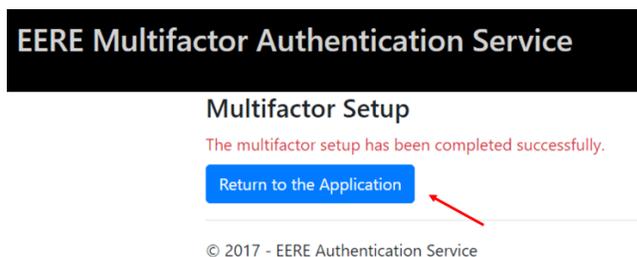


15. Once **SMS, Phone App**, or both are verified click the **Finish** button.

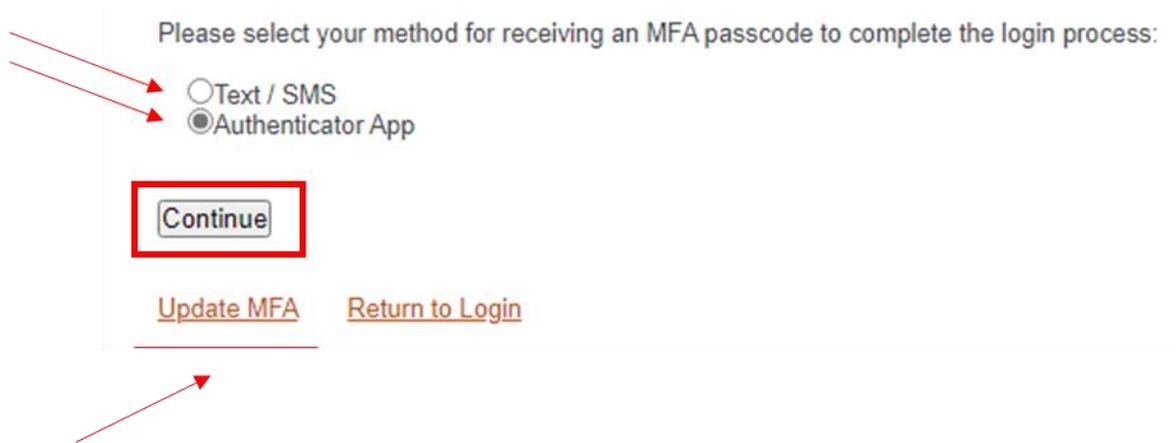
A screenshot of the 'EERE Multifactor Authentication Service' setup interface. At the top, a black header contains the text 'EERE Multifactor Authentication Service' in white. Below the header, the text 'Welcome to the Multifactor Authentication Setup' is displayed. A red warning message states 'You must complete the setup in 19:30 mins.' and a blue instruction says 'Select and configure the delivery methods you would like to use.' There are two main configuration sections. The first is for 'SMS', which is checked and has a 'Set as Default' button. Below it, the phone number '(+1) 1234567899' is shown with a 'SMS Verified' status and a 'Redo Setup' button. The second section is for 'Phone App', which is checked and marked as the 'Default Delivery Method'. Below it, 'Google' is listed as the authentication app with an 'App Verified' status and a 'Redo Setup' button. At the bottom, there are three buttons: 'Finish' (blue), 'Select Finish to Save and return to your application.' (grey), and 'Cancel' (red). A red arrow points to the 'Finish' button. The footer contains the copyright notice '© 2017 - EERE Authentication Service'.

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.

A screenshot of the 'EERE Multifactor Authentication Service' 'Multifactor Setup' completion screen. A black header contains the text 'EERE Multifactor Authentication Service' in white. Below the header, the text 'Multifactor Setup' is displayed. A red message states 'The multifactor setup has been completed successfully.' Below this is a blue button with the text 'Return to the Application'. A red arrow points to the 'Return to the Application' button. The footer contains the copyright notice '© 2017 - EERE Authentication Service'.

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.



Please select your method for receiving an MFA passcode to complete the login process:

Text / SMS

Authenticator App

Continue

[Update MFA](#) [Return to Login](#)

The screenshot shows a user interface for selecting an MFA method. The title is "Please select your method for receiving an MFA passcode to complete the login process:". There are two radio button options: "Text / SMS" and "Authenticator App". The "Authenticator App" option is selected. Below the options is a "Continue" button, which is highlighted with a red box. At the bottom, there are two links: "Update MFA" and "Return to Login". Red arrows point to the radio buttons and the "Continue" button. A red arrow also points to the "Update MFA" link.

*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.*