User Guide: How to Set Up Multifactor Authentication

Multifactor Authentication (MFA) requires users to log in with the correct User ID, password, and another form of authentication, such as identity confirmation through an authentication app or an email address. Access to Fannie Mae browser-based applications requires the use of MFA.

This guide explains how to set up the MFA verification method during first-time login, including:

- Set Up Third-Party Authenticator Method
- Set Up Text Message Method
- Set Up Automated Phone Call Method
- Set Up Email Method
- Success Notification

The user must setup at least one MFA verification method to access Fannie Mae systems.

> **Notes:**
>
> The available MFA verification methods depend on the MFA Package selected by your Corporate Administrator.
>
> To skip MFA setup, select **Skip for Now.** This option is only available until the Enforcement Date selected by your Corporate Administrator.

The table below provides an overview of all available MFA verification methods:

MFA Method	Description
Third-Party Authenticator App	Retrieve a 6-digit code through a third-party application such as DUO, Google or Microsoft Authenticator. The user is prompted to enter the code into the interface.
Text Message	Receive a 6-digit code via text message. The user is prompted to enter the code into the interface.
Automated Phone Call	Receive a 6-digit code via an automated phone call. The user is prompted to enter the code into the interface.
Email	Receive an email with a 6-digit code at the email address registered with Fannie Mae. The user is prompted to enter the code into the interface.

Set Up Third-Party Authenticator App

This section explains how to set up the third-party authenticator method. When utilizing this method, the user retrieves a 6-digit code through a third-party app such as Duo, Google or Microsoft Authenticator and is prompted to enter the code into the interface.

1. Log in to a Fannie Mae browser-based application for the first time.
2. After providing the correct User ID and password, the user will be prompted to set up the MFA verification method via the Help Us Protect Your Account panel
3. If not yet done, please download and install the desired third-party authenticator app from the App Store or Google Play on your device.

> **Note:** The following third-party apps have been tested and validated: Google Authenticator, Microsoft Authenticator, and Duo.

4. Click the **Set Up** button next to **Third-Party Authenticator App.**

5. Enter the **Device Nickname**, then select **Continue.**

> **Note:** Nickname will auto populated but user can update the Nickname.
>
> The **Device Nickname** can contain numbers, letters, and the following special characters: space ( ), asterisk (*), hyphen (-), underscore (_), and apostrophe ('). The maximum length is 30 characters.
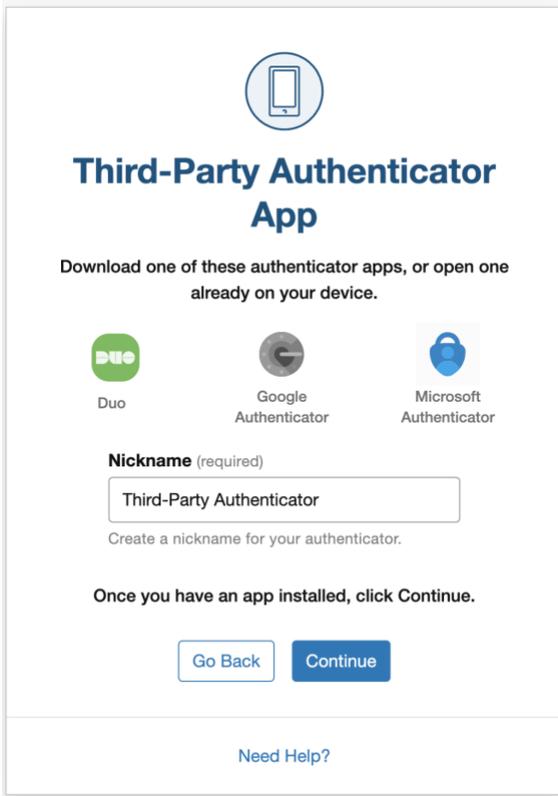
6. Scan the QR code using the third-party authenticator app to pair the app, then select **Continue.**
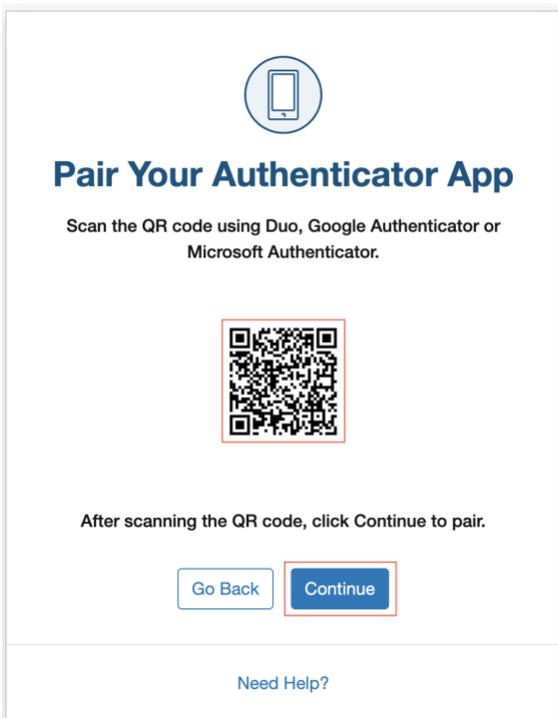
7. Enter the 6-digit code from the third-party authenticator app in the boxes, then select **Verify.**

Note: User has 6 attempts to enter the valid code. If the code expires, enter the new code from the third-party authenticator app.

8. Once successfully registered, the user has the option to:
   - Set third-party authentication app as the preferred authentication method
   - Continue to Application
   - Set up more verification methods
   - Manage MFA settings

Notes:

To set this method as your preferred verification method, click the **Set as preferred verification method** checkbox. The **Set up more verification methods** option will be unavailable once you click the **Set as preferred verification method** checkbox. To set up more verification methods, you can always select **Manage MFA Settings**.

Refer to **User Guide: How to Manage Multifactor Authentication** for more information on how to manage MFA settings.

9. The user will receive a confirmation email upon receipt of the success notification.

Set Up Text Message Method

This section explains how to set up the text message authentication method. When utilizing this method, the user receives a 6-digit code in a text message to their device. Corporate Admin from your organization should select Package 2 to make Text Message available.

1. Log in to a Fannie Mae browser-based application for the first time
2. After providing the correct User ID and password, the user will be prompted to set up the MFA verification method via the Help Us Protect Your Account panel

3. Click the **Set Up** button next to **Text Message.**

4. United States of America will be the default selection in the **Country** field, click in the Country field to open the drop down to change the country, enter the **Mobile Phone Number**, edit the **Device Nickname** if desired, then click **Continue.**

Notes:

The **Mobile Phone Number** must be a valid phone number for the **Country** selected. This field can only contain numbers.

The **Device Nickname** can only contain numbers, letters, and the following special characters: space ( ), asterisk (*), hyphen (-), underscore (_), and apostrophe ('). The maximum length is 30 characters.

---

5. Enter the 6-digit code sent via text message to the mobile phone number entered in **Step 2** in the boxes, then select **Verify.**

> **Note:** User has 6 attempts to enter the valid code. The code is valid for 15 minutes. If the code expires, select **Resend Code** to receive new code. There is a daily limit of 10 codes for texts and phone calls.

6. Once successfully registered, the user has the option to:
   - Set text message as the preferred authentication method

- Continue to Application
- Set up more verification methods
- Manage MFA settings

> **Notes:**
>
> To set this method as your preferred verification method, click the **Set as preferred verification method** checkbox. The **Set up more verification methods** option will be unavailable once you click the **Set as preferred verification method** checkbox. To set up more verification methods, select **Manage MFA Settings**.
>
> Refer to **User Guide: How to Manage Multifactor Authentication** for more information on how to manage MFA settings.
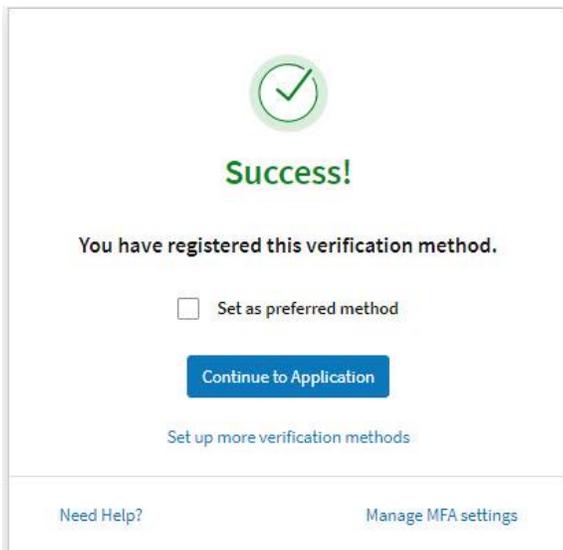
7. The user will receive a confirmation email upon receipt of the success notification.

Set Up Automated Phone Call Method

This section explains how to set up the automated phone call authentication method. When utilizing this method, the user receives a 6-digit code via an automated phone call and is prompted to enter the code into the interface.

1. Log in to a Fannie Mae browser-based application for the first time
2. After providing the correct User ID and password, the user will be prompted to set up the MFA verification method via the Help Us Protect Your Account panel
3. Click the **Set-Up** button next to **Automated Phone Call.**

4. United States of America will be the default selection in the **Country** field, click in the Country field to open the drop down to change the country, enter the **Mobile Phone Number**, edit the **Device Nickname** if desired, then click **Continue.**

Notes:

The **Phone Number** must be a valid phone number for the **Country** selected. This field can only contain numbers.

The **Device Nickname** can only contain numbers, letters, and the following special characters: space ( ), asterisk (*), hyphen (-), underscore (_), and apostrophe ('). The maximum length is 30 characters.

5. Enter the 6-digit code sent via automated phone call to the phone number entered in **Step 2** in the boxes, then select **Verify.**

Note: User has 6 attempts to enter the valid code. The code is valid for 15 minutes. If the code expires, select **Resend Code** to receive new code. There is a daily limit of 10 codes for texts and phone calls.

7. Once successfully registered, the user has the option to:

- Set phone call as the preferred authentication method
- Continue to Application
- Set up more verification methods
- Manage MFA settings

Notes:

To set this method as your preferred verification method, click the **Set as preferred verification method** checkbox. The **Set up more verification methods** option will be unavailable once you click the **Set as preferred verification method** checkbox. To set up more verification methods, select **Manage MFA Settings**.

Refer to **User Guide: How to Manage Multifactor Authentication** for more information on how to manage MFA settings.
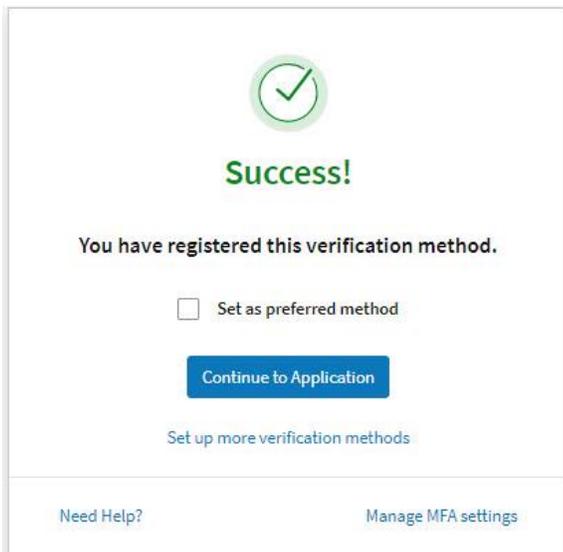
8. The user will receive a confirmation email upon receipt of the success notification.

Set Up Email Method

This section explains how to set up the email authentication method. When utilizing this method, the user receives a 6-digit code at the email address registered with Fannie Mae and is prompted to enter the code into the interface. Fannie Mae registered email will be available for all the users.

1. Log in to a Fannie Mae browser-based application for the first time.
2. After providing the correct User ID and password, the user will be prompted to set up the MFA verification method via the Help Us Protect Your Account panel
3. Click the **Set Up** button next to **Email.**

4. Enter the 6-digit code sent to the email address registered with Fannie Mae in the boxes, then select **Verify.**

Note: User has 6 attempts to enter the valid code. The code is valid for 15 minutes. If the code expires, select **Resend Code** to receive new code.

8. Once successfully registered, the user has the option to:
   - Set email as the preferred authentication method
   - Continue to Application
   - Set up more verification methods
   - Manage MFA settings

Notes:

To set this method as your preferred verification method, click the **Set as preferred verification method** checkbox. The **Set up more verification methods** option will be unavailable once you click the **Set as preferred verification method** checkbox. To set up more verification methods, select **Manage MFA Settings**.

Refer to **User Guide: How to Manage Multifactor Authentication** for more information on how to manage MFA settings.

9. The user will receive a confirmation email upon receipt of the success notification.

Success Notification

The Success Notification panel is returned upon completion of a registration method(s). After the initial selection of an authentication method the user can establish additional verification methods by clicking on the **Set up more verification methods link**. The **Set as preferred method** checkbox defines the registered method as the default authentication method. The user can opt to go directly to the application by clicking the **Continue to Application** button. The use can also click the Manage MFA settings link to add an additional MFA verification method, delete MFA verification method, change preferred MFA verification method, and change device nickname.