The Commonwealth of Kentucky

TEAM KENTUCKY®

CABINET FOR HEALTH AND FAMILY SERVICES

Quick Reference Guide

MFA Management (Setup and Removal)

Last Updated: 05.14.2026

Contents

MFA Management (Setup / Reset)

Multi-Factor Authentication (MFA) adds an extra layer of security to your account by requiring more than one method of authentication. This guide will walk you through the steps to set up MFA using various authenticator applications, alternate email addresses, and registered mobile numbers. MFA may be triggered while you are creating your account, or you can set it up manually from security settings. This user guide demonstrates the steps to set up or reset MFA manually.

To review the steps for MFA that are triggered while creating a new account on KYID, please refer to the **Create Account User Guide**.

There are **mandatory** fields marked with an **asterisk** (*****). These fields must be completed to proceed.

1. Setting up MFA

This section provides step-by-step instructions for setting up multifactor authentication (MFA) for your KYID account.

You can enable MFA using an alternate email address, a registered mobile number, or one of the supported authenticator applications available within the KYID portal. The methods listed below can be used to secure your KYID account with multifactor authentication:

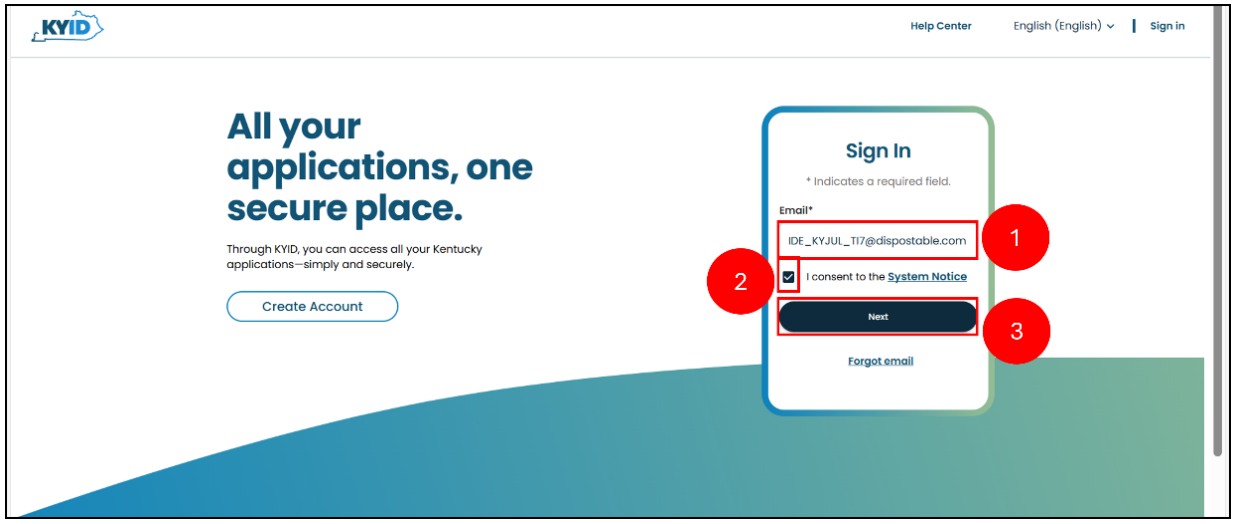
Setting up MFA through Various Methods

MFA enhances account security by requiring users to verify their identity using two or more authentication factors. The following subsections walk you through each method and offer clear steps to safeguard a smooth setup process.

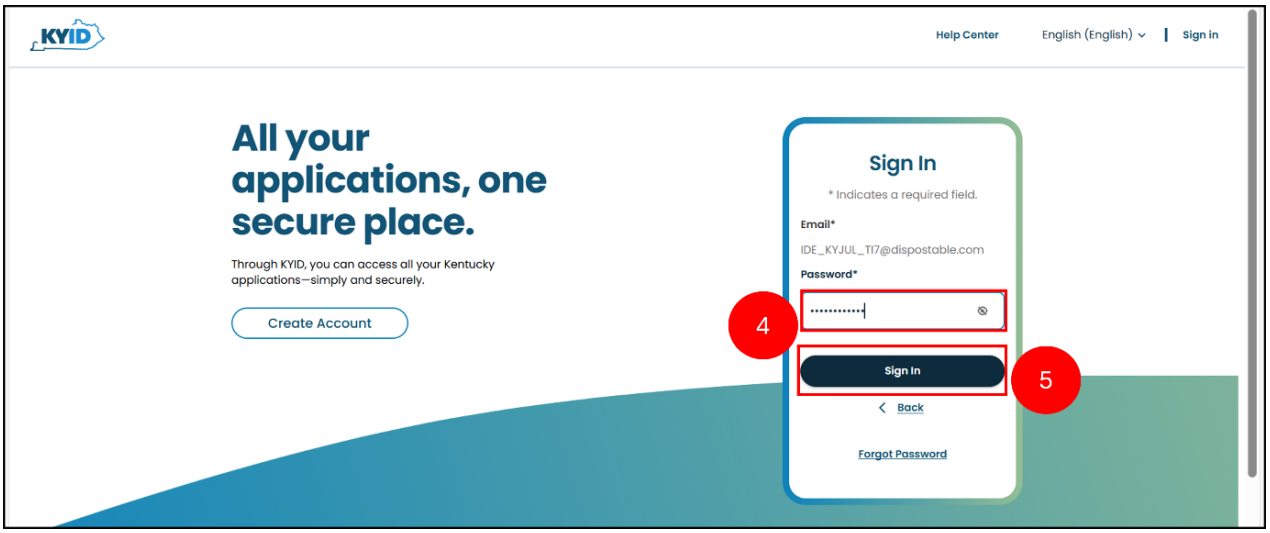
- **MFA Application**: The MFA application method uses an authenticator app (such as ForgeRock Authenticator, Microsoft Authenticator, Google Authenticator, and Symantec VIP) installed on your mobile device or desktop. After registering on the app, you will receive one-time passcodes (OTPs) that you enter during sign-in as the second authentication factor.
- **Mobile Number Authentication**: In this method an SMS, or a voice call is used to deliver verification codes to your registered mobile number.
- **How to update MFA (self-enroll method)**: The self-enrollment option allows you to change or update your MFA method at any time. This is useful if you change devices, switch phone numbers, or want to enhance your security by selecting a different authentication factor.

1.1 Pre-requisite MFA – Signing in KYID for the first time

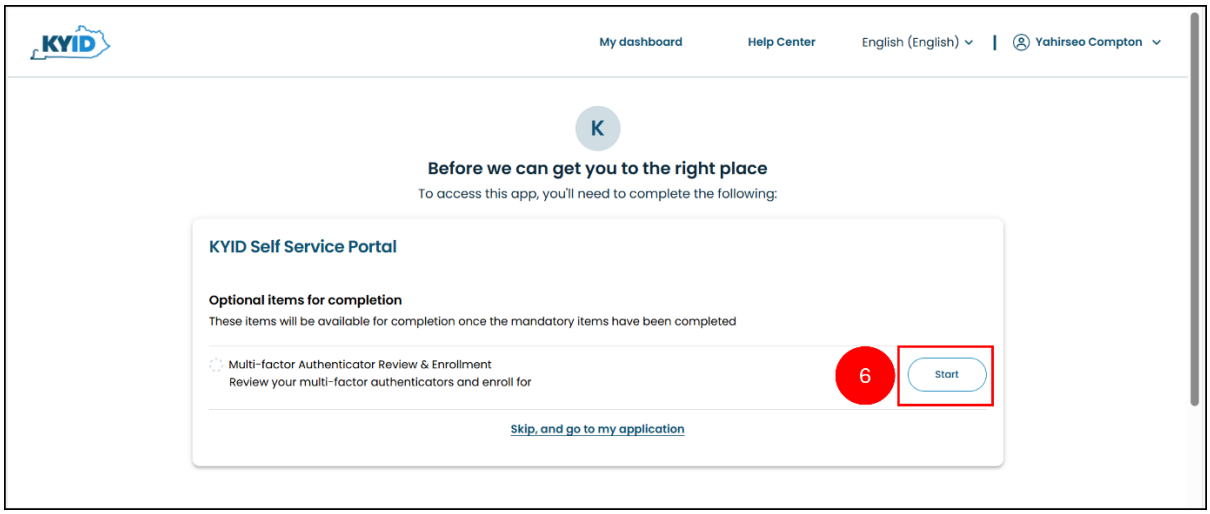
1. When logging in to KYID for the first time, enter your registered email address in the **Email*** field on the **KYID** sign in screen.
2. Select the **I consent to the System Notice** checkbox.
3. Click **Next** to proceed.



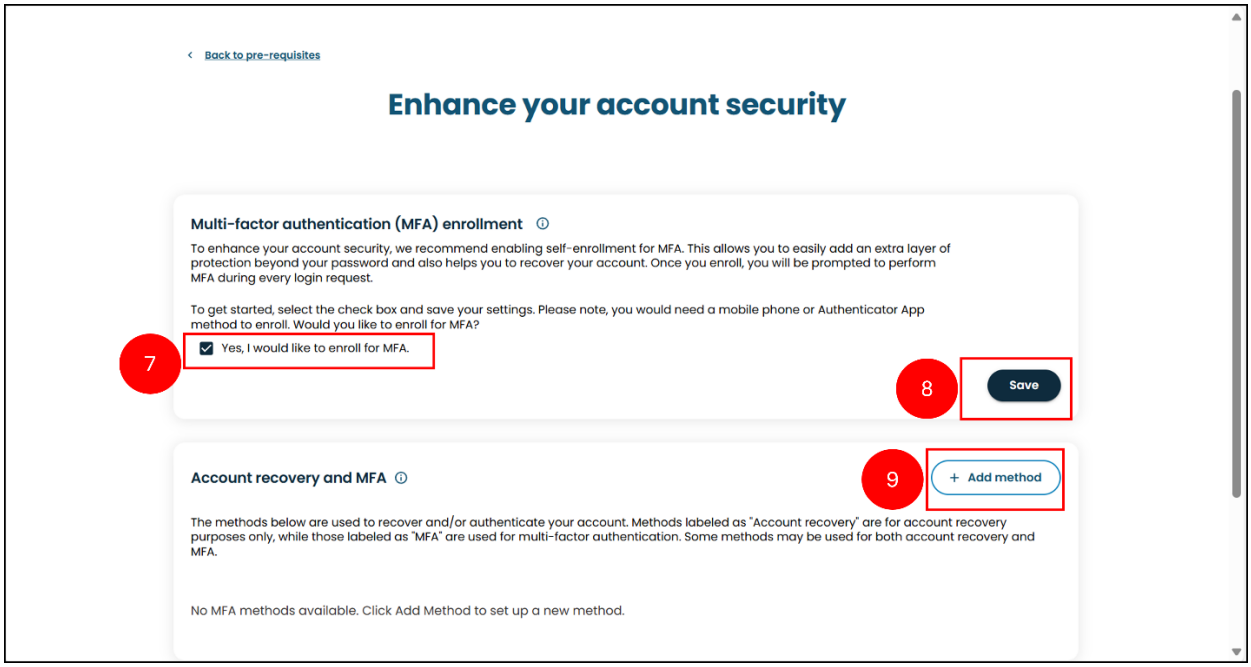
4. Enter your password in the **Password** field.
5. Click **Sign in** to proceed.



6. The **Before we can get you to the right place** screen appears. Click **Start** to proceed.

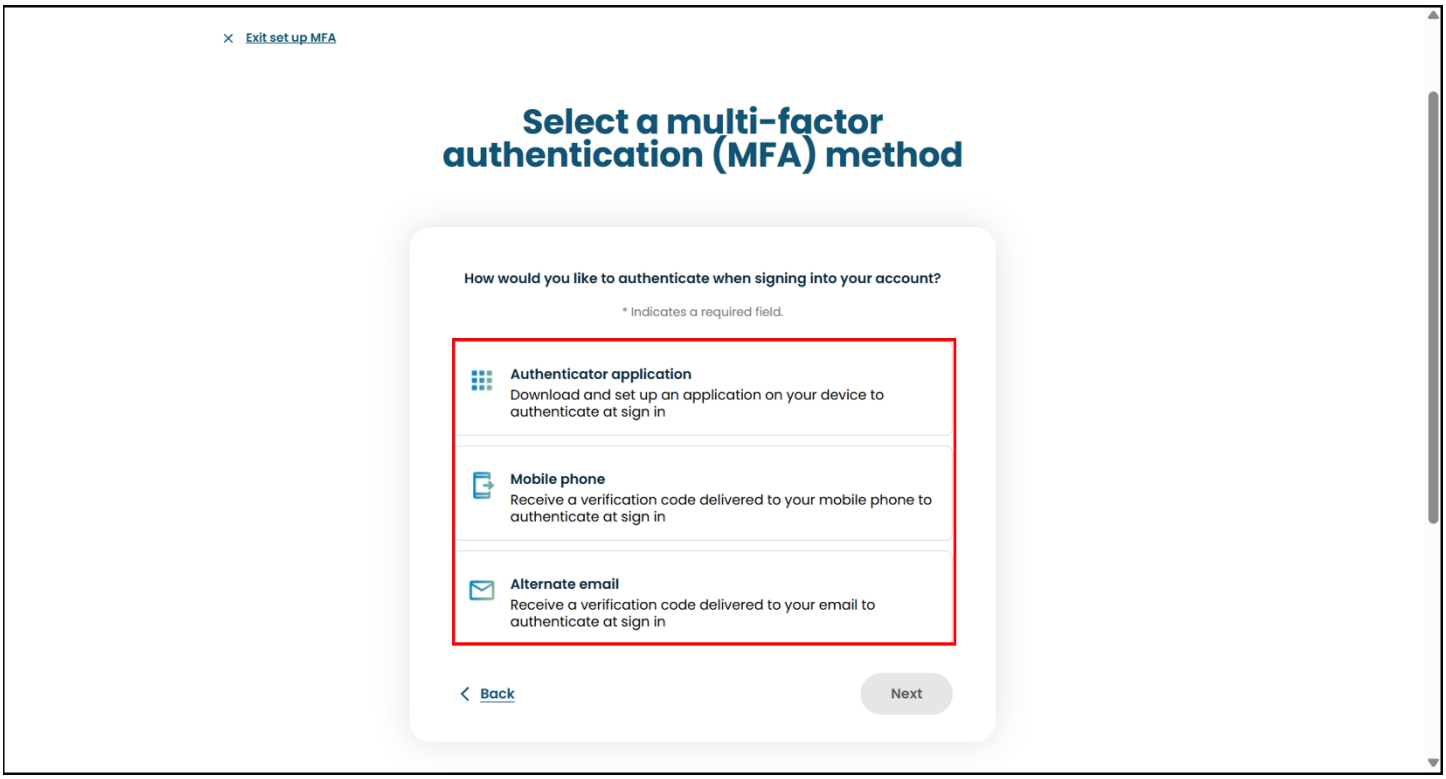


7. The **Enhance your account security** screen appears. Scroll down to the **Multi-factor authentication (MFA) enrollment** section to set up MFA. Select the **Yes, I would like to enroll for MFA** checkbox.
8. Click **Save** to confirm the selection.
9. Under the **Account recovery and MFA** section, click the **+Add method** to add account recovery methods.



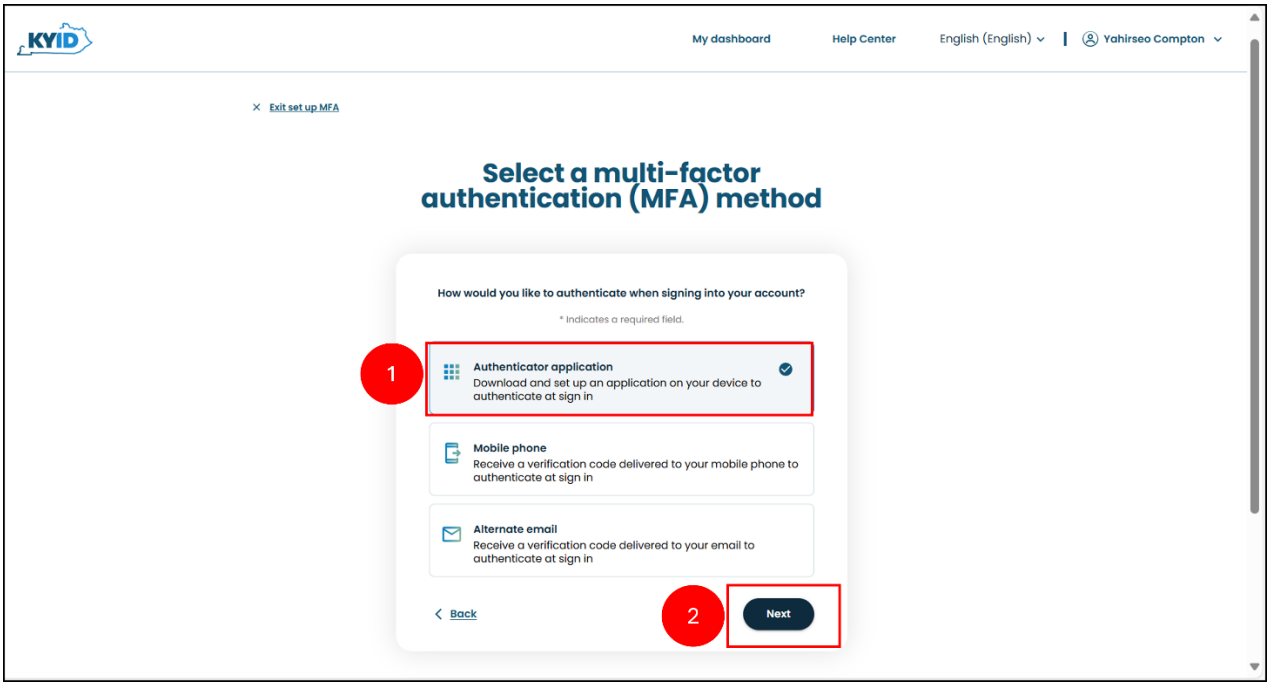
The **Select a multi-factor authentication (MFA) method** screen appears. Your available MFA options are role-based, meaning the options may not be available to you based on the type of information you access. MFA methods include:

1. Authenticator application
2. Mobile phone
3. Alternate Email.

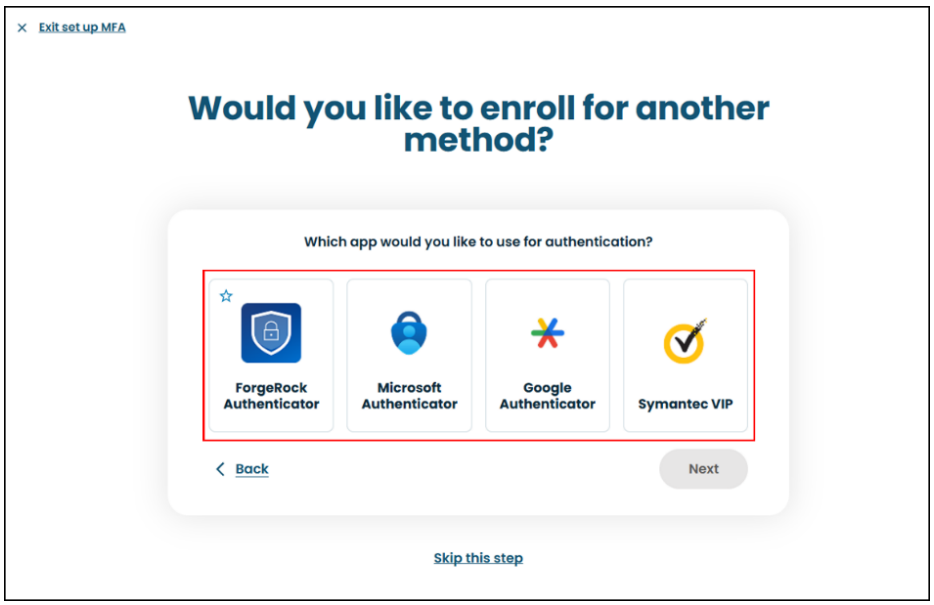


1.1.2. Authenticator application option

1. To set up your account recovery using the authenticator app, select the **Authenticator application** checkbox.
2. Select **Next** to proceed.



On the **Would you like to enroll for another method?** screen, you will see four authentication applications available for selection. To continue, choose one of the applications.



Please note: You can only have one push notification method and one one-time password (OTP) method configured at a time. For instance, if you have set up ForgeRock Push Notifications, you cannot enable Google Push Notifications simultaneously. Similarly, if Google OTP is active, ForgeRock OTP cannot be configured at the same time. To switch to a different MFA method, first remove the existing method from the **Account Recovery and MFA** section, then select and add your preferred application.

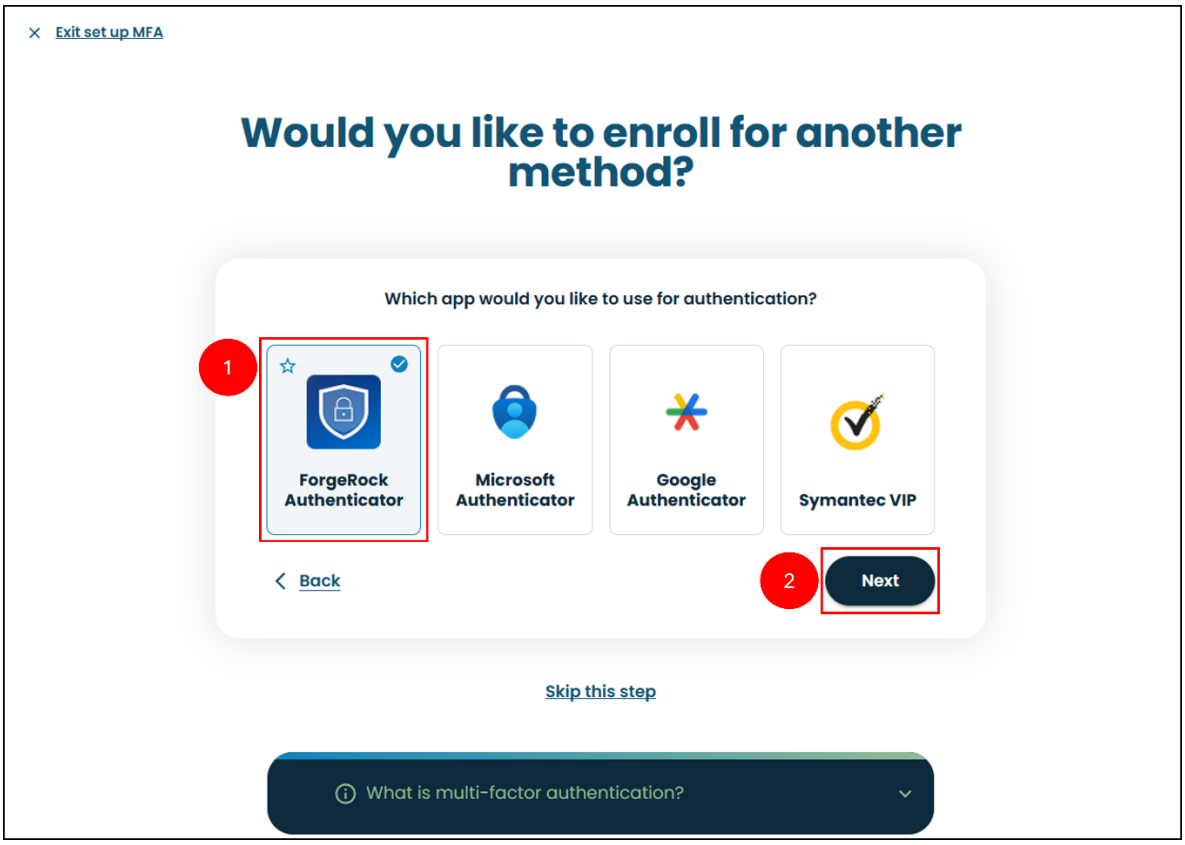
Prerequisites: Before you begin, confirm you have access to your primary email, and a mobile device with one of the following authenticator apps installed:

A. ForgeRock Authentication application
B. Microsoft Authentication application
C. Google Authentication application
D. Symantec VIP application

A. ForgeRock Authenticator

The **ForgeRock Authenticator** app enhances your KYID account security by generating one-time passcodes or sending push notifications to your device. During the MFA setup process, you can configure the app to authenticate using either push notifications or time-based codes. Once registered through the KYID portal, ForgeRock Authenticator will be available as an authentication method. When signing in, you may be prompted to verify your identity using a push notification or a code generated by the ForgeRock app.

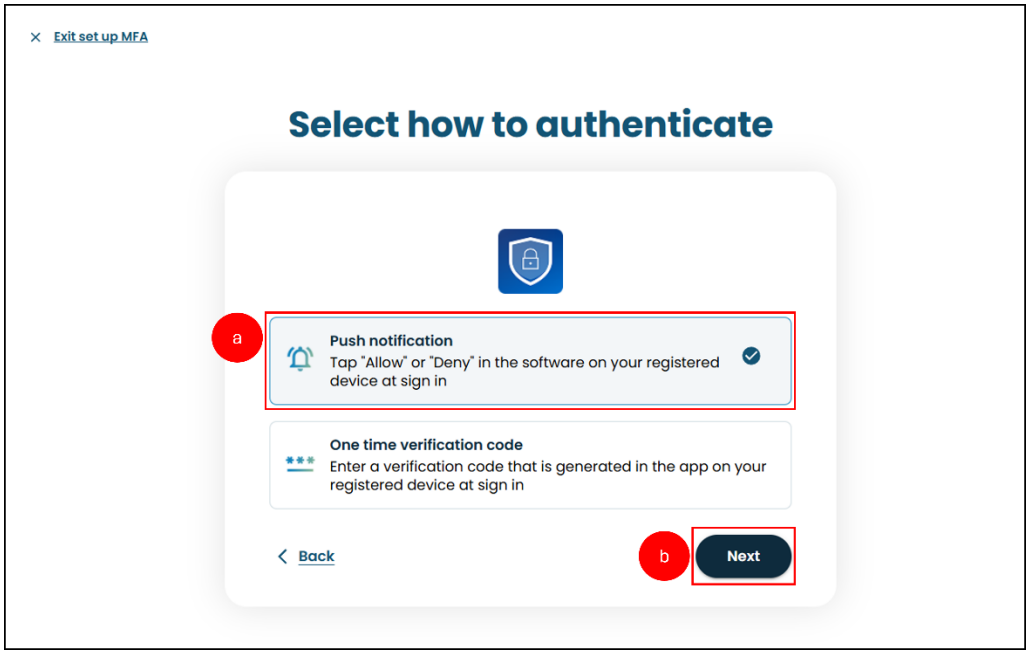
1. Select **ForgeRock Authenticator** on the **Would you like to enroll for another method?** screen.
2. Click **Next** to proceed.



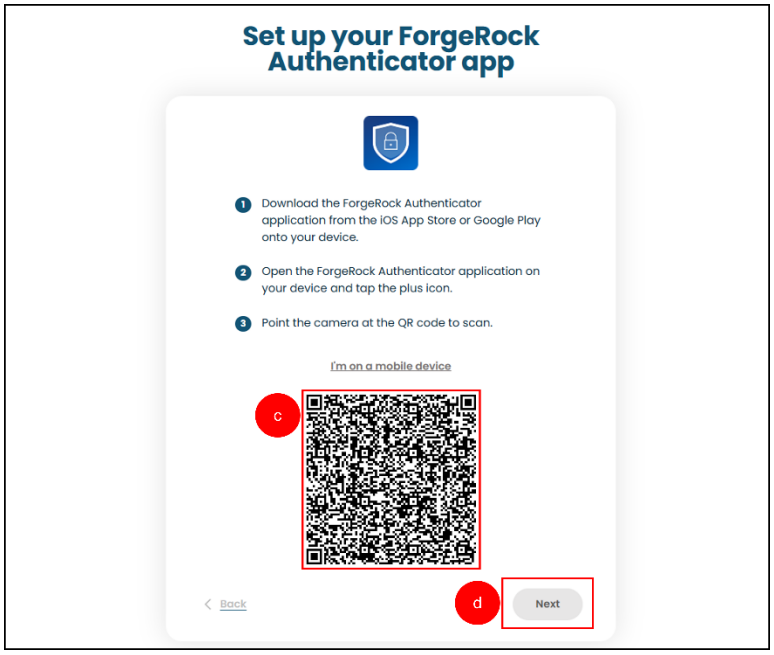
On the **Select how to authenticate** screen, two checkboxes are available **Push notification** checkbox or the **One-time verification code**. **Push notification** checkbox can be selected to receive a notification on the mobile device with the options **Allow** or **Deny**. You can select **Allow** on your mobile device and proceed with the authentication or you can select **Deny** if you do not wish to proceed with this authentication method. **One time verification code** checkbox can be selected to receive a verification code that is generated in the app on your registered device.

2.1. Push notification option:

a. Select **Push notification** checkbox.
b. Select **Next**.

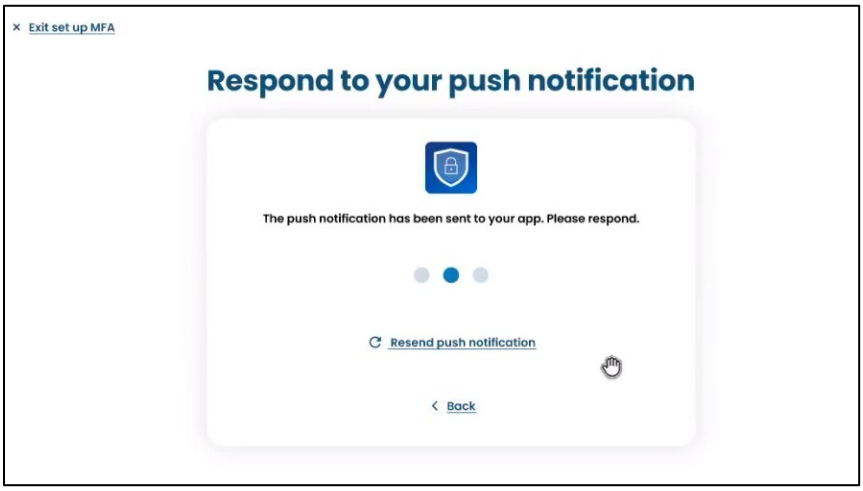


c. Follow the instructions displayed on the **Set up your ForgeRock Authenticator App** screen to download the ForgeRock application on your device. Scan the **QR code** displayed on the screen. **Do not scan the QR code in this document.**
d. Once the scan is successful, the **Next** button with be enabled. Click the **Next** button to continue.



Please note: If you are performing the authentication steps on a mobile device, then you may select the I'm on a mobile device link that is displayed above the QR code. A pop-up will appear trying to open the ForgeRock Authenticator application. Click **Allow** on the pop-up message. Then, click **Accept** in the ForgeRock Authenticator application. Reopen your browser on your mobile device and click next and continue from Step d.

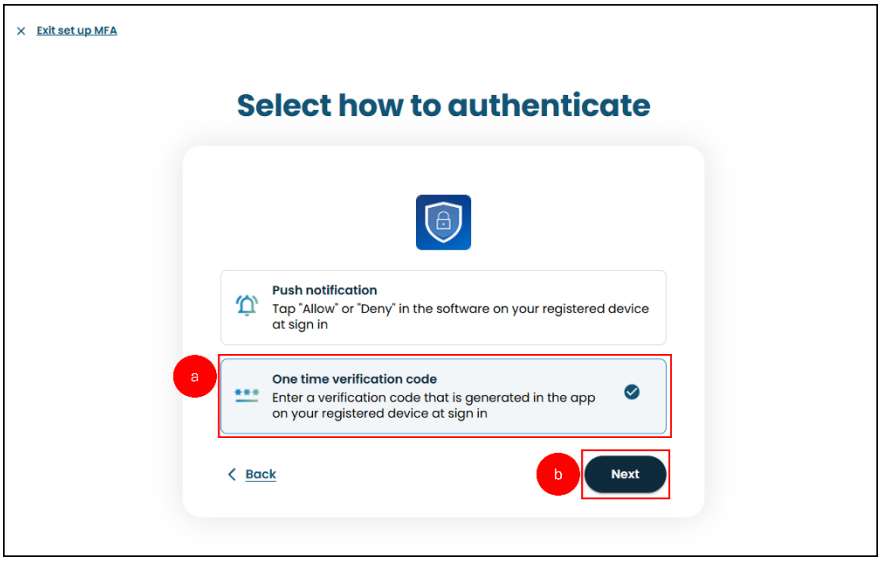
e. On the **Respond to your push notification** screen, the system displays a loading screen, waiting for you to respond to the notification sent on your mobile app. Click **Allow** on the mobile device to proceed.



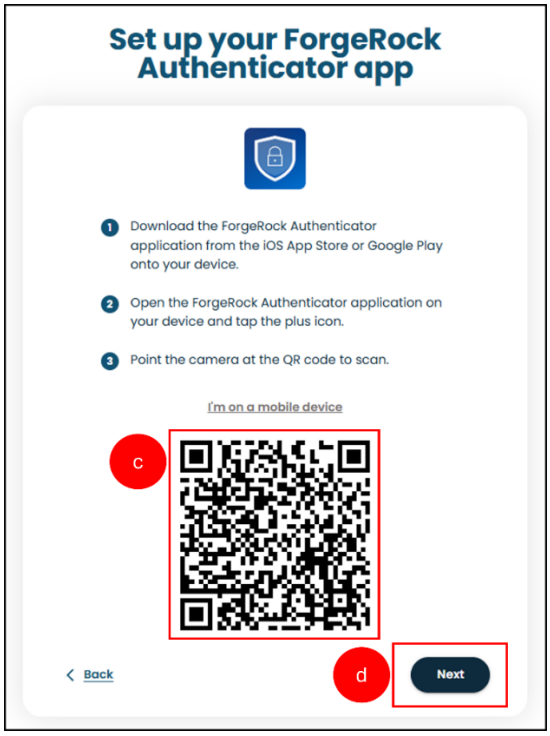
Please note: In case you did not select any response, then **Resend push notification** link will be enabled. You can select this link to resend the notification or select the **Back** link to go to the previous screen to change the authentication method.

2.2. One time verification code option:

a. Select **One time verification code** checkbox.
b. Select **Next**.

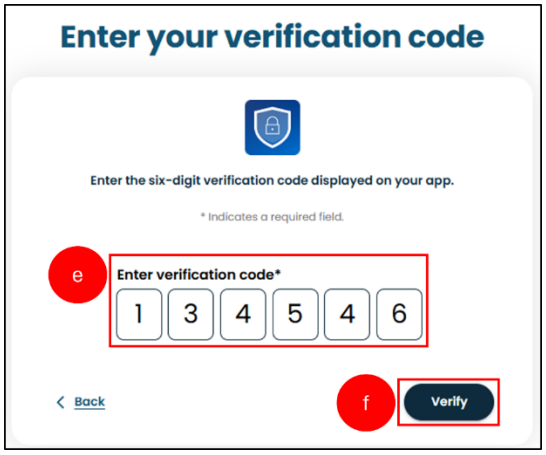


c. Follow the instructions displayed on the **Set up your ForgeRock Authenticator App** screen to download the ForgeRock application on your device. Scan the **QR code** displayed on the screen. **Do not scan the QR code in this document.**
d. Once the scan is successful, the **Next** button with be enabled. Click the **Next** button to continue.



Please note: If you are performing the authentication steps on a device, then you may select the I'm on a mobile device link that is displayed above the QR code. A pop-up will appear trying to open the ForgeRock Authenticator application. Click **Allow** on the pop-up message. Then, enter the code shown in the ForgeRock Authenticator application into the verification field on your mobile device and continue with the Step f.

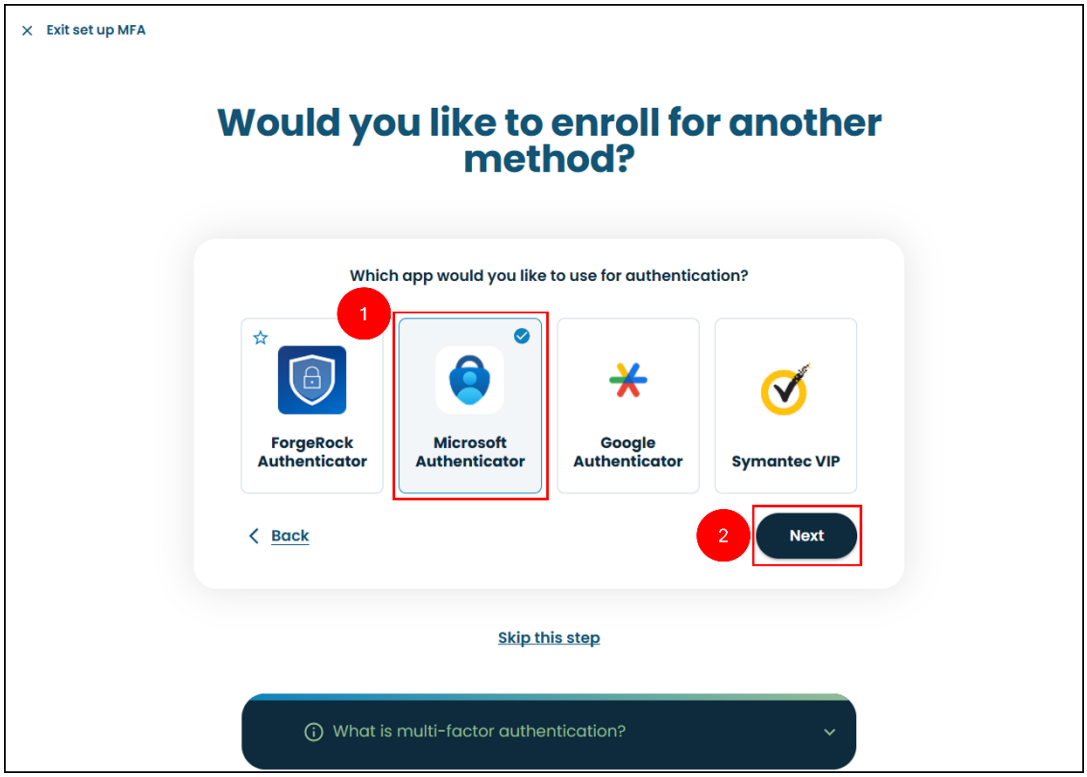
e. Enter the six-digit code sent to the device in the **Enter verification code*** field.
f. Click **Verify** to complete the ForgeRock MFA setup.



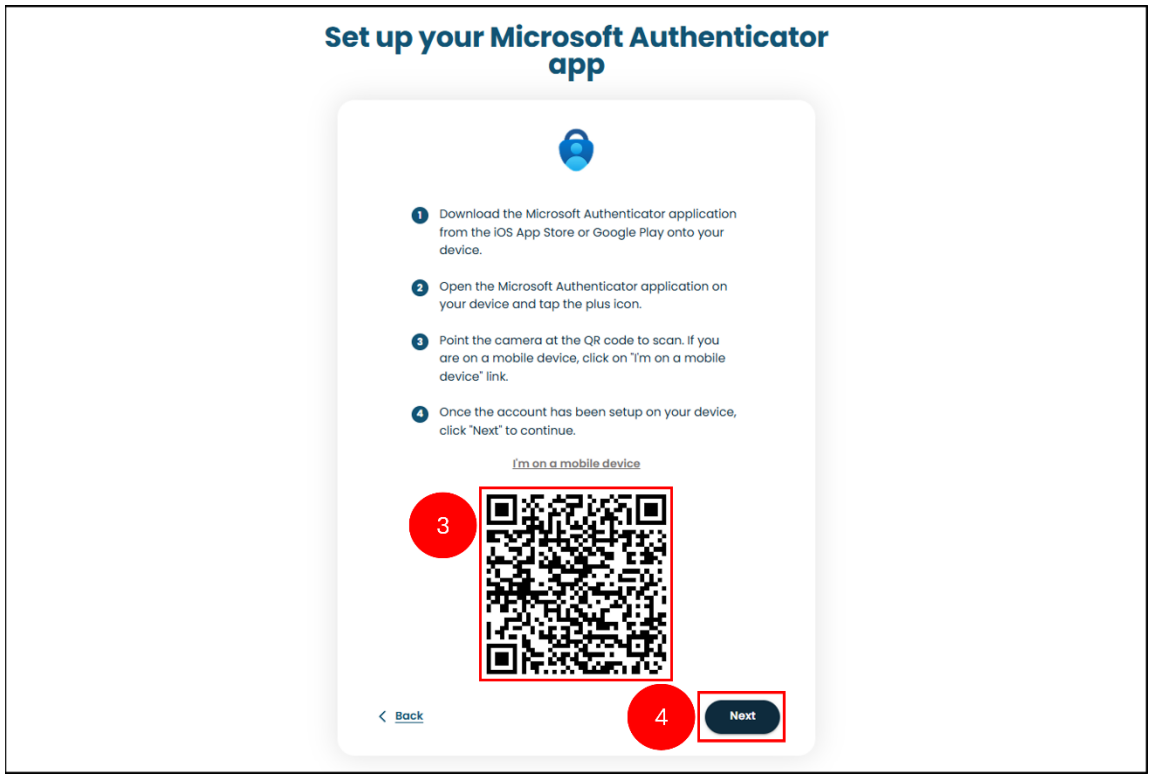
B. Microsoft Authenticator

The **Microsoft Authenticator** app provides secure account access by generating time-based codes or sending push notifications to your device. By following the steps below, you can set up the app by scanning a QR code and completing verification with either a push notification or a code during the MFA configuration process.

1. Select **Microsoft Authenticator** app on the **Would you like to enroll for another method?** screen.
2. Click **Next** to proceed.

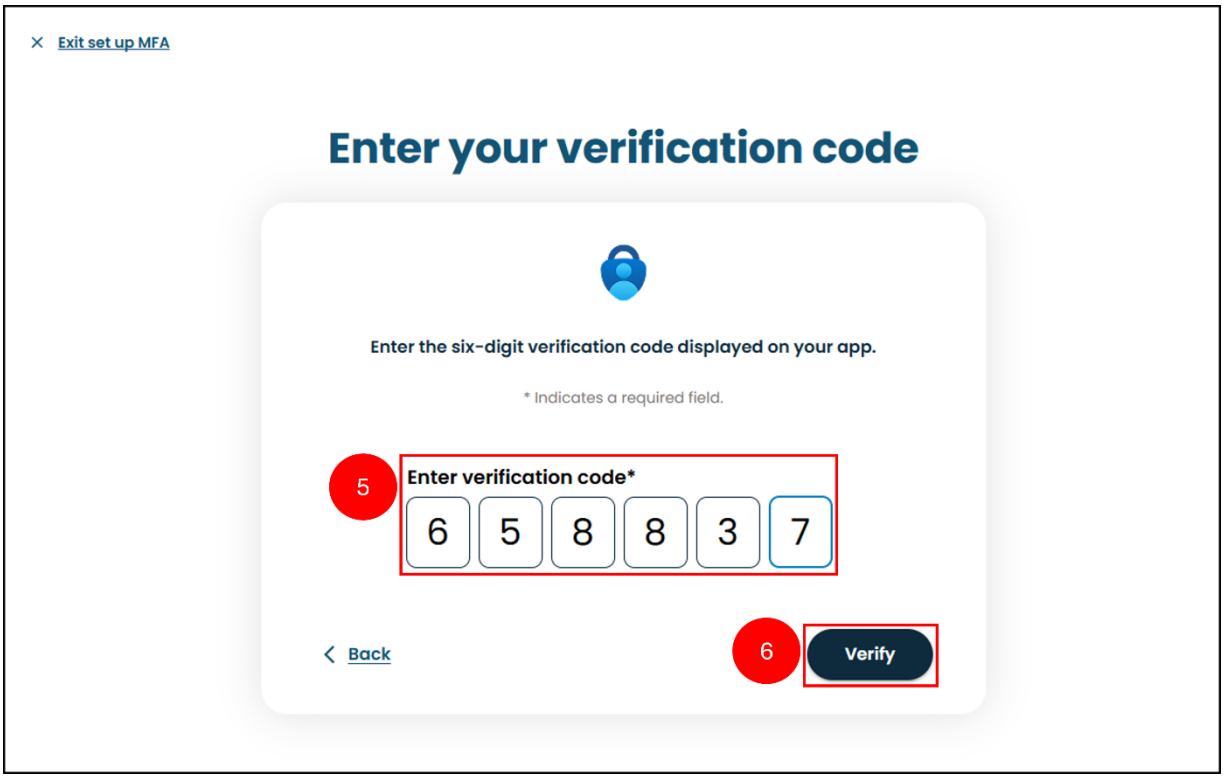


3. Follow the instructions displayed on the **Set up your Microsoft Authenticator App** screen to download the Microsoft application on your device. After the app is installed and ready, scan the **QR code** displayed on the **Set up your Microsoft Authenticator app** screen with the help of your mobile device. **Do not scan the QR code in this document.**
4. Once the scan is successful, the **Next** button with be enabled. Click the **Next** button to continue.



Please note: If you are performing the authentication steps on a device, then you may select the **I'm on a mobile device** link that is displayed above the QR code. A pop-up will appear trying to open the Microsoft Authenticator application. Click **Allow** on the pop-up message. Then, enter the code shown in the Microsoft Authenticator application into the verification field on your mobile device and continue with the Step 4.

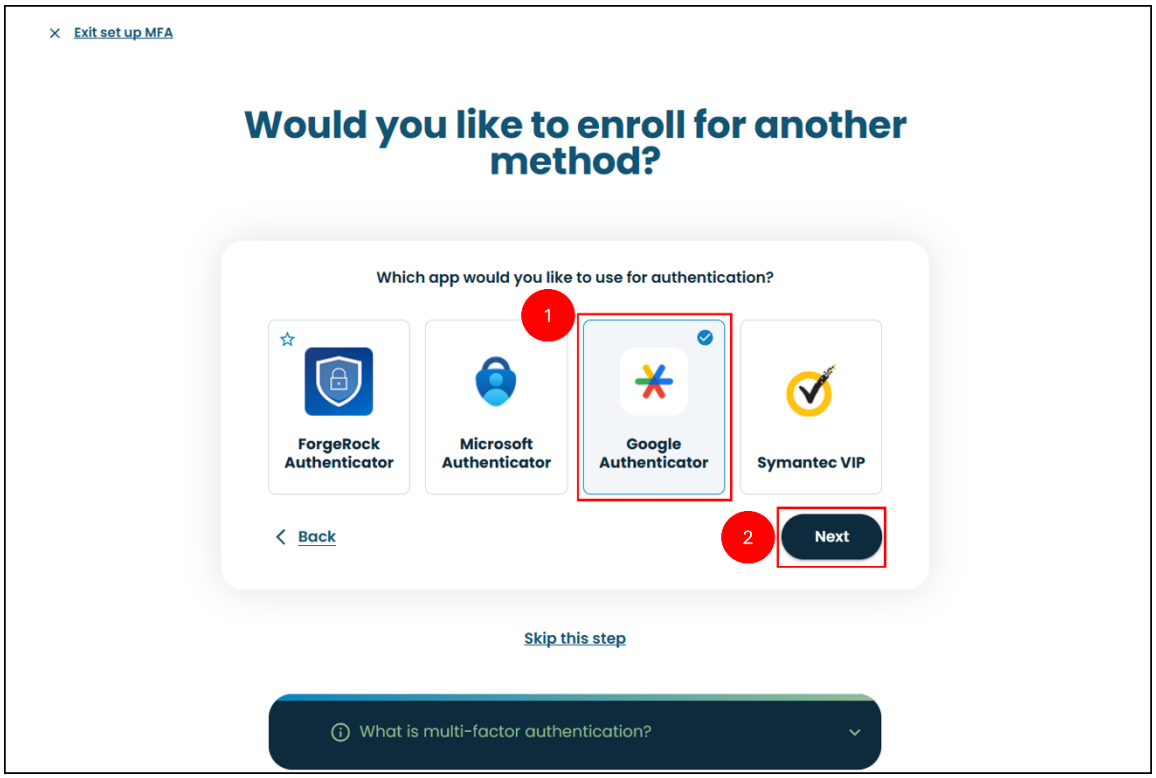
5. In the **Enter the verification code*** field enter the code displayed on the authenticator app on your mobile device.
6. Click **Verify** to proceed and complete setup of your Microsoft MFA.



C. Google Authenticator

The **Google Authenticator** app secures your account by generating time-based, one-time passcodes on your device. By following the steps below, you can set up the app by scanning a QR code or entering the code displayed during the MFA configuration process.

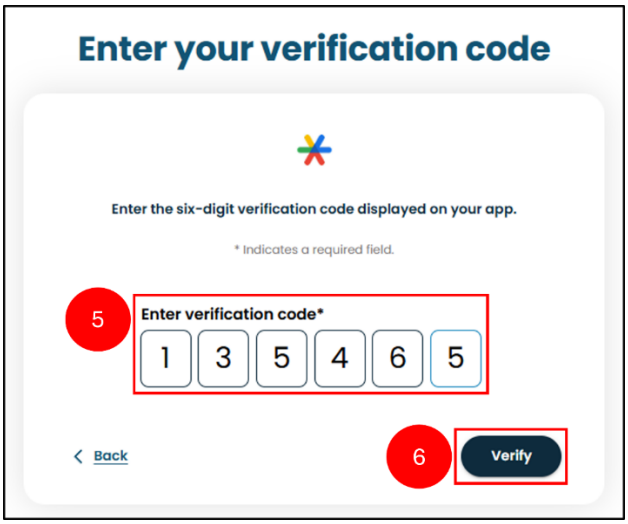
1. Select **Google Authenticator** app on the **Would you like to enroll for another method?** screen.
2. Click **Next** to proceed.



3. Follow the instructions displayed on the **Set up your Google Authenticator App** screen to download the Google application on your device. After the app is installed and ready, scan the **QR code** displayed on the **Set up your Google Authenticator app** screen with the help of your mobile device. **Do not scan the QR code in this document.**
4. Once the scan is successful, the **Next** button with be enabled. Click the **Next** button to continue.

Please note: If you are performing the authentication steps on a device, then you may select the **I'm on a mobile device** link that is displayed above the QR code. A pop-up will appear trying to open the Google Authenticator application. Click **Allow** on the pop-up message. Then, enter the code shown in the Google Authenticator application into the verification field on your mobile device and continue with the Step 4.

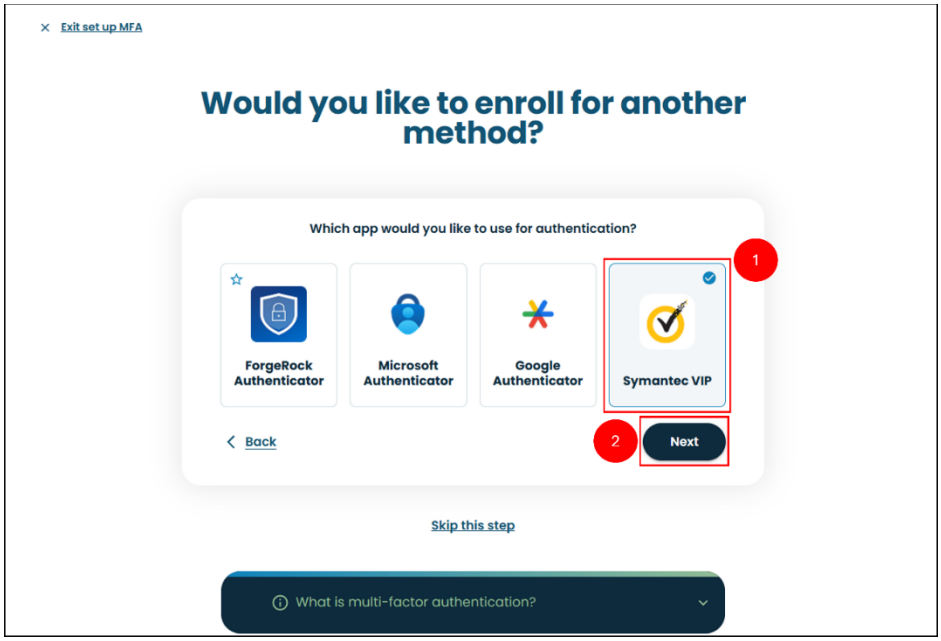
5. In the **Enter the verification code*** field enter the code displayed on the authenticator app on your mobile device.
6. Click **Verify** to proceed.



D. Symantec VIP

The Symantec VIP authentication app enhances account security by generating unique, time-based security codes on your device. By following the steps below, you can set up the app by registering your device's Credential ID and entering two consecutive codes from the app during the MFA configuration process.

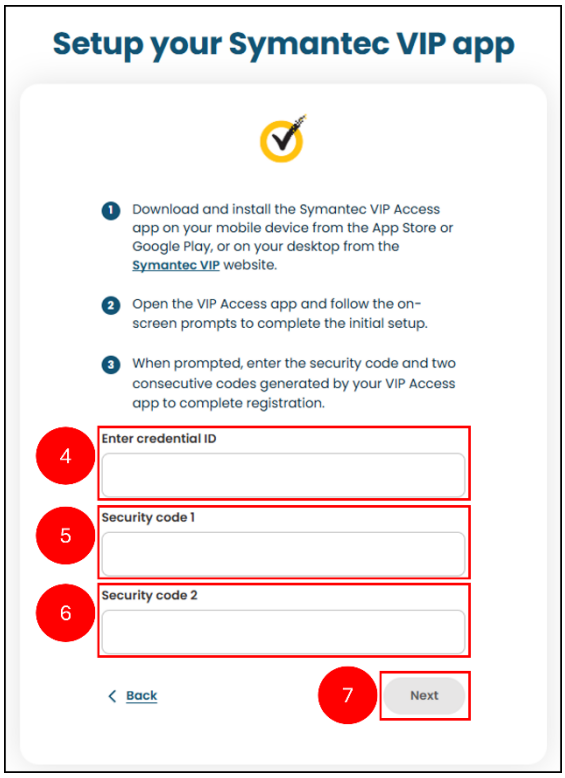
1. Select **Symantec VIP** on the **Select an authenticator application** screen.
2. Click **Next**.



Please note: If you have not yet installed the VIP Access app onto your machine or device, then you must download and install it by visiting the Symantec website at https://vip.symantec.com/ for the desktop version, the App Store for iPhone and iPad devices, or the Google Play for Android devices.

3. Open the **Symantec VIP** app and locate your unique **Credential ID** and the **Security Code**.

4. Enter the **Credential ID**, which is displayed in the **VIP Access** app, in the **Enter credential ID** field on the **Setup your Symantec VIP app** screen in KYID.
5. Generate two consecutive security codes in the **VIP Access** app. Enter the first security code in the **Security Code 1** field.
6. Wait for the code to refresh, then enter the second security code in the **Security Code 2** field.
7. Click **Next** to submit the codes and complete the Symantec VIP MFA setup.



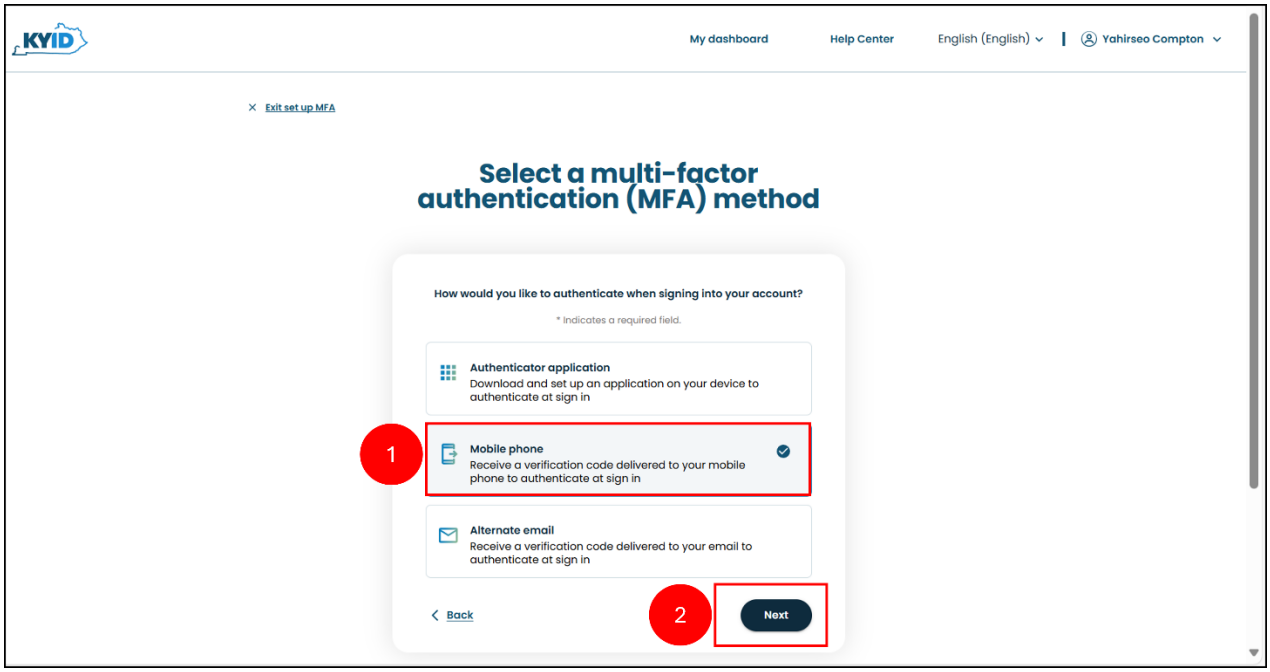
Please note: The Security Code refreshes every thirty (30) seconds. If the second code expires before you click the **Next** button, enrollment will fail. You must then return to the VIP Access application to receive two new valid **Security Codes**.

1.1.3. Mobile Number Authentication

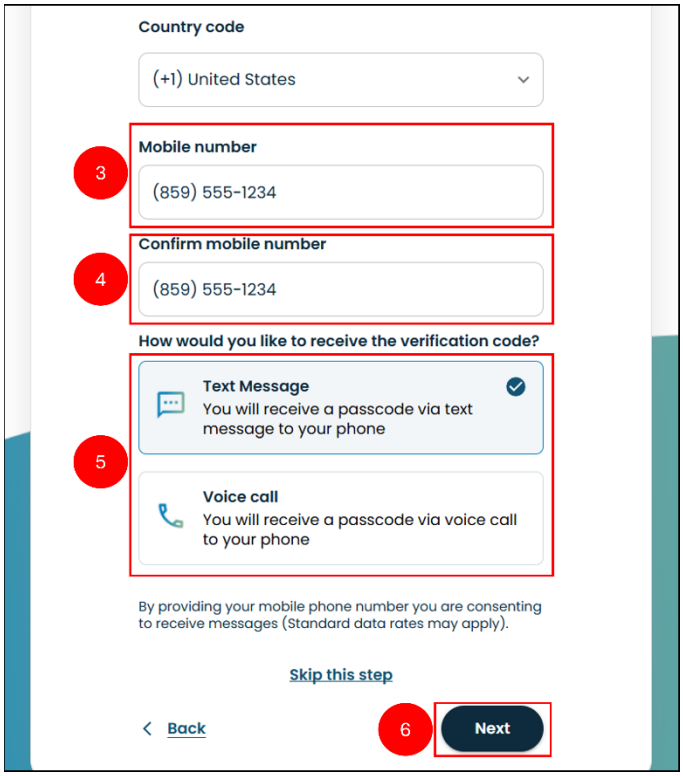
Mobile number authentication can be set up as an additional security measure for your KYID account. Once you register your mobile number in the KYID portal, it becomes available as an authentication method by default. Each time you sign in to KYID, you may be prompted to verify your identity using a code sent to your registered mobile number. This method will become optional when you set up MFA via an authentication application.

Follow the steps below to authenticate your account via email address.

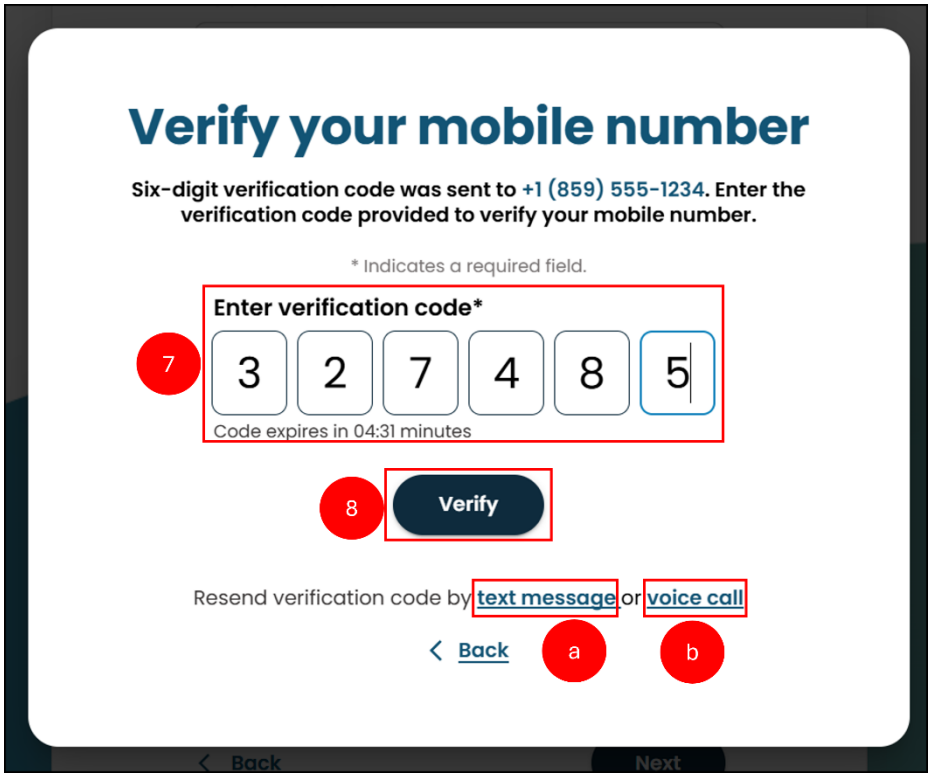
1. Select **Mobile phone** on the **Select a multi-factor authentication (MFA) method** screen.
2. Click **Next**.



3. Enter your mobile number in the **Mobile number** field.
4. Re-enter the same mobile number in the **Confirm mobile number** field.
5. To verify your mobile number, select one of the following options to receive the verification code on your selected mobile number:
    - **Text message**: Receive a code via SMS.
    - **Voice call**: Receive a code through a phone call.
6. Click **Next**.



7. Enter the six-digit code in the **Enter verification code*** field. **Note that the code expires after five minutes**. You must enter the code before it expires.
8. After entering the code, click **Verify** to proceed. Upon successful verification, a success message appears. If you need a new code sent to your mobile device:
    a. Select the **text message** link to receive a new code via text message in case the code expires or you have not received it.
    b. Select the **voice call** link in case you prefer to receive the code via a voice call.

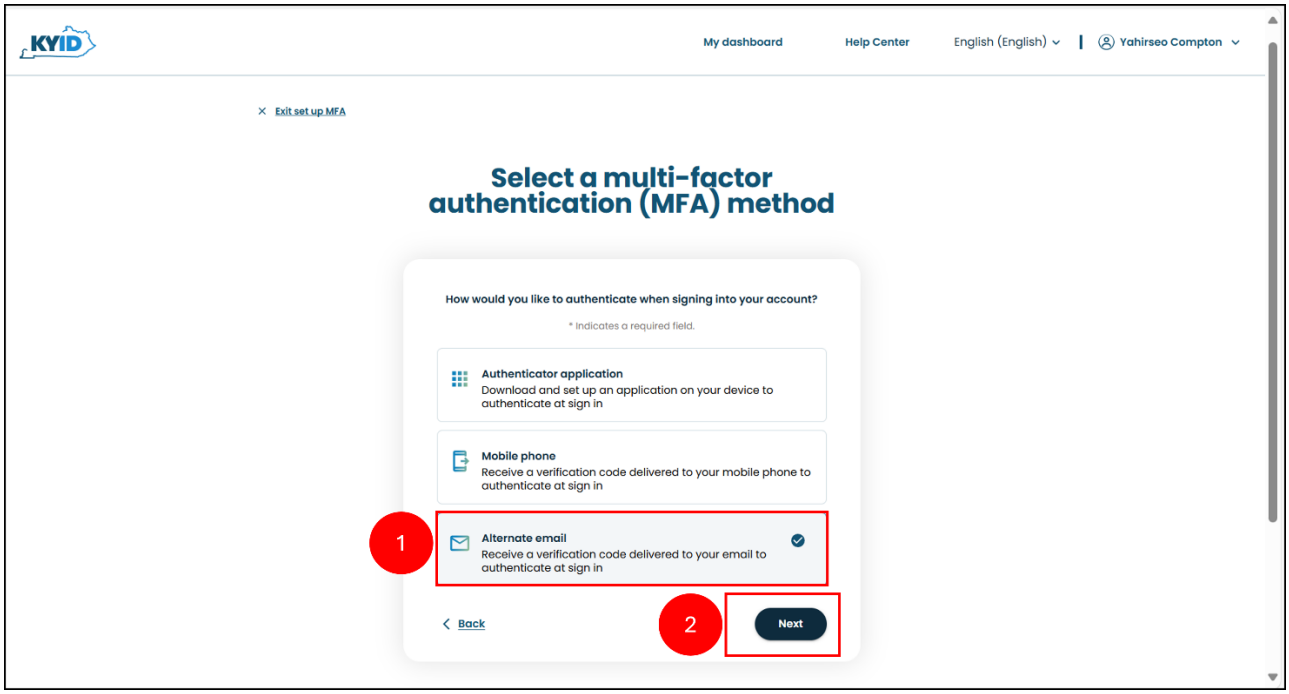


1.1.4. Alternate Email Authentication

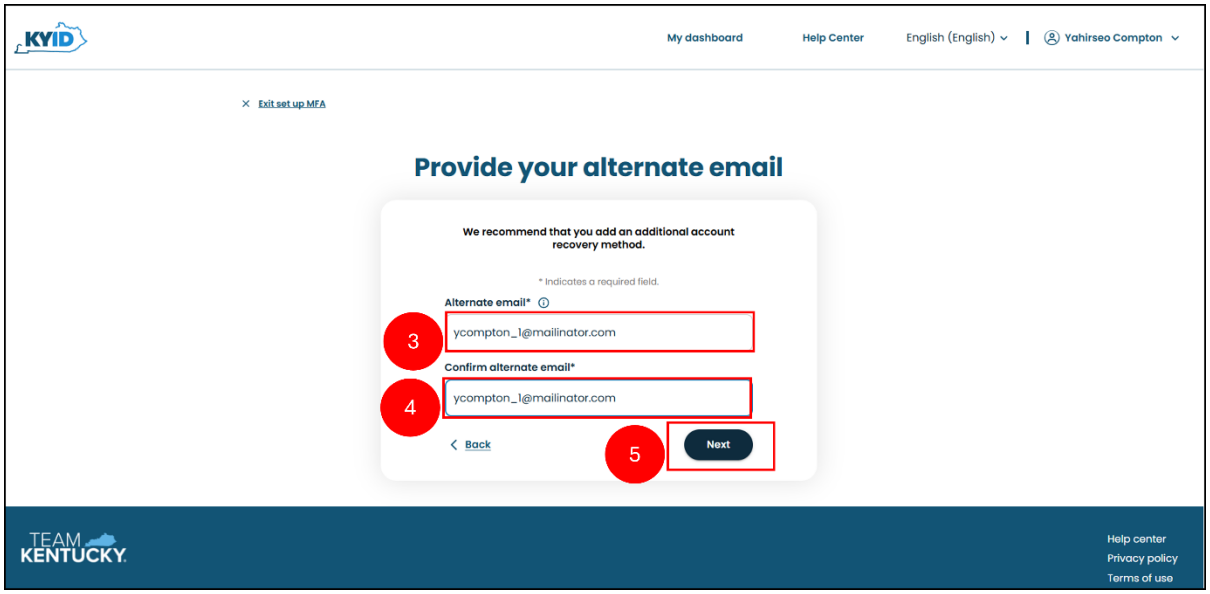
Email authentication is automatically configured when you create your KYID account. By default, your primary email address serves as the primary authentication method for your KYID account. This authentication step will be prompted each time you sign in to KYID using your registered email address. Below are the steps to add an Alternate email address to your KYID account for verification.

Follow the steps below to authenticate your account via your alternate email address.

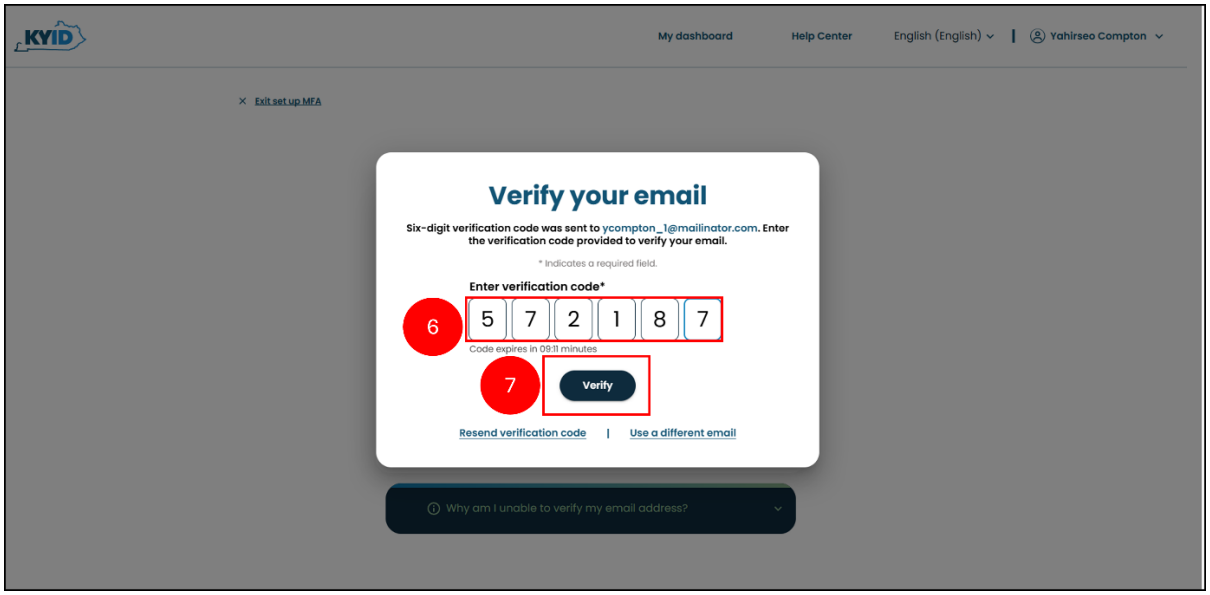
1. To set up your account recovery using an alternate email, select the **Alternate email** option.
2. Click **Next** to proceed.



3. Enter your alternate email address in the **Alternate email*** field.
4. Re-enter your alternate email address in the **Confirm alternate email*** field.
5. Click **Next** to proceed.



6. On the **Verify your email** popup, enter the code in the **Enter verification code*** field.
7. Click **Verify** to complete the alternate email MFA setup.

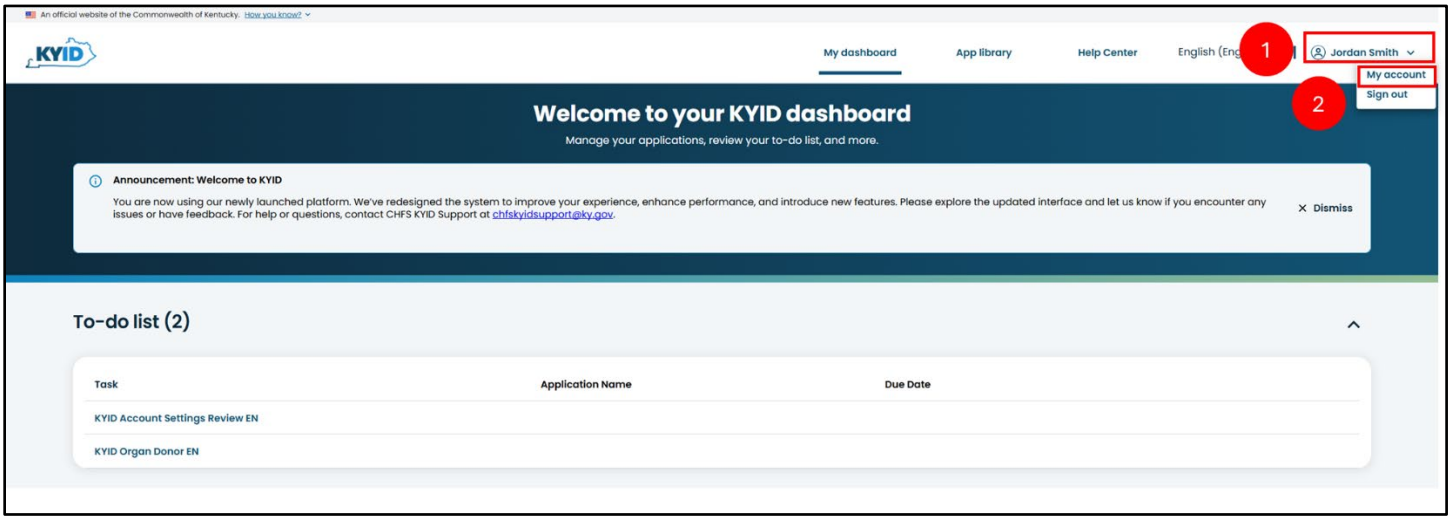


Please note: The code sent to your alternate email will be valid for 10 minutes. You can select **Resend verification code** link to resend the code in case not received.

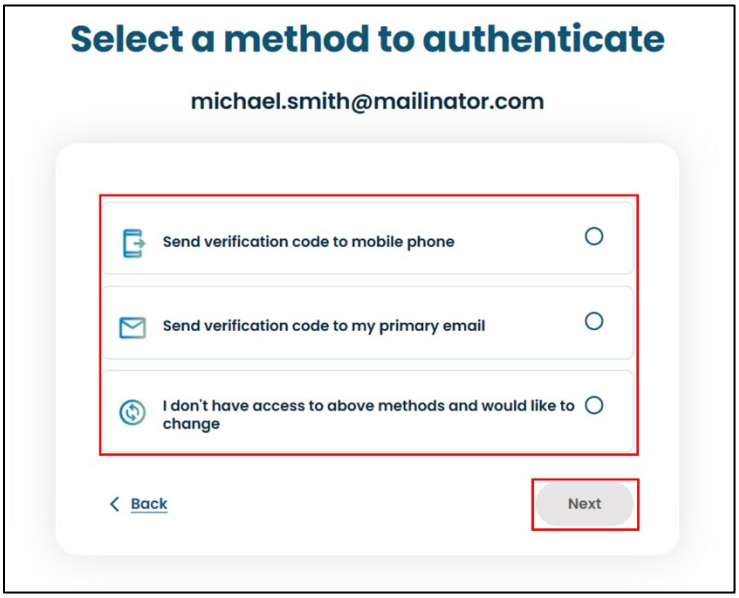
1.2. Setting up MFA (Self Enrollment Method)

You can also set up MFA via applications from the **Login and Security** tile on the **My account** screen.

1. Select the dropdown arrow next to your profile on the top right corner of the **My dashboard** screen.
2. Select **My account** from the menu.

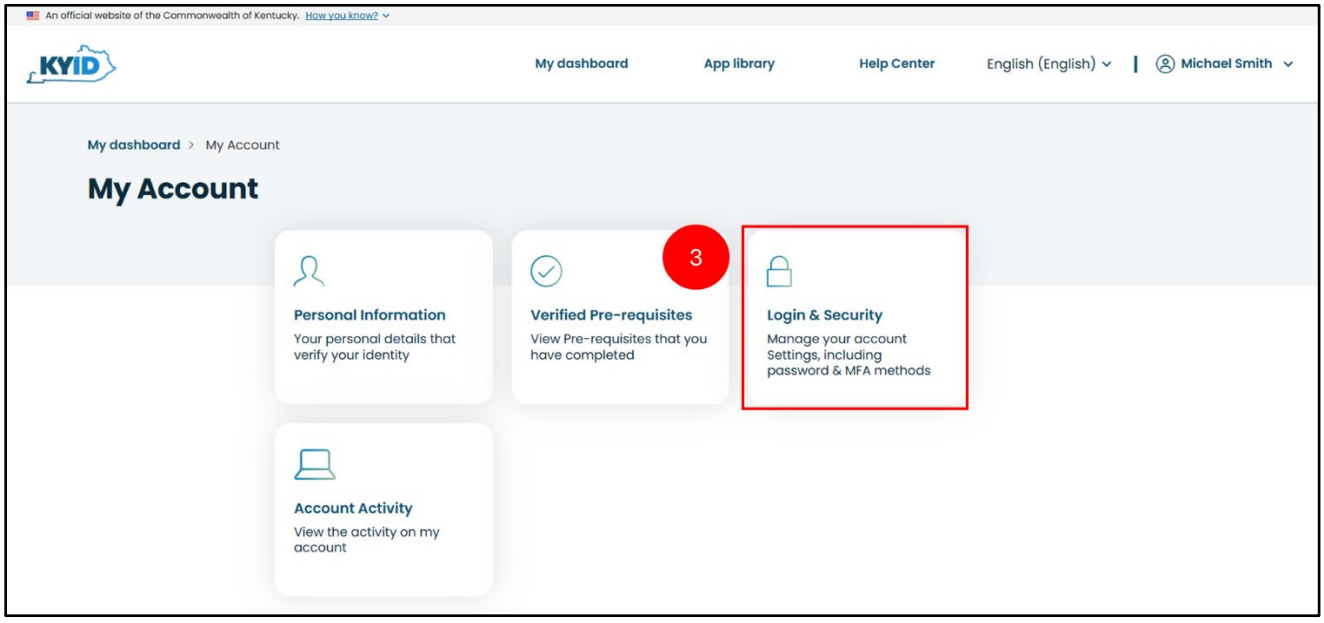


If this is your first time accessing the **My account** page, you are prompted to authenticate with either your mobile phone or through your primary email address tied to your KYID account. A verification code will be sent to either your mobile phone through text message or voice call or it will be sent to your primary email address. Select the option you desire and enter the verification code to continue.



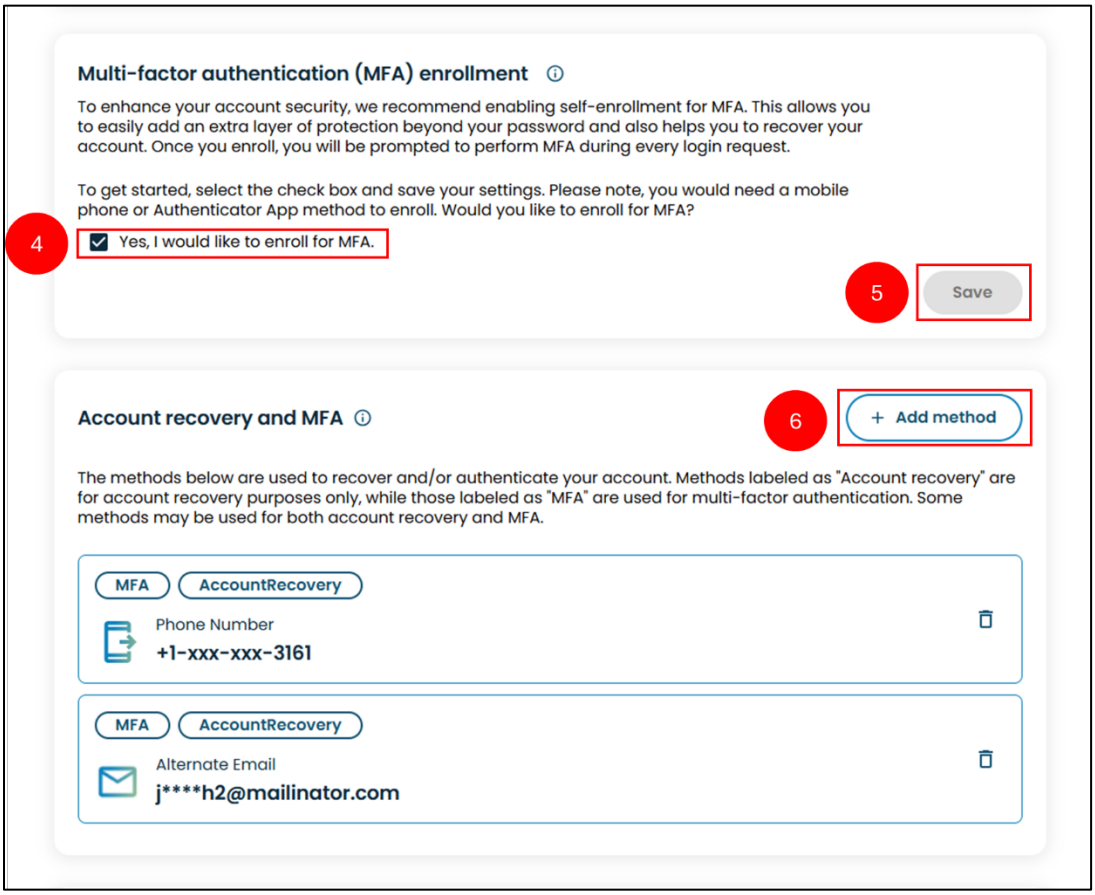
Please note: If you do not have access to the above methods and would like to change, you may verify your identity through Identity verification or by entering a verification code sent to your primary and alternate emails.

3. Select the **Login & Security** tile on the My account screen.



On the **Login & Security** screen, you will be able to update **Login details**, set up **MFA via Multi-factor authentication (MFA) enrollment**, access **Account recovery and MFA** options, and **Account Management** options.

4. Scroll down to the **MFA via Multi-factor authentication (MFA) enrollment** section to set up MFA. Select the **Yes, I would like to enroll for MFA** checkbox.
5. Click **Save** to confirm the selection.
6. In the **Account recovery and MFA** section, click **+ Add method** button and then follow the same steps in the **1.1.2. Authenticator application option** section of this QRG.

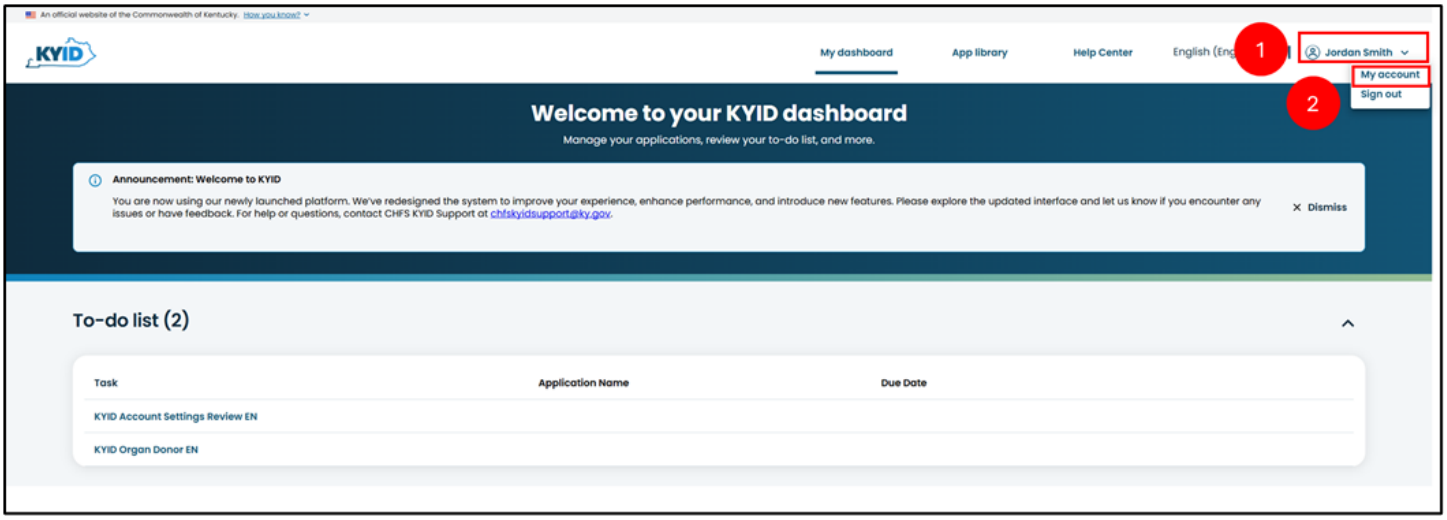


Please note: Users can add up to three (3) mobile phone numbers for verification and up to four (4) authenticator applications

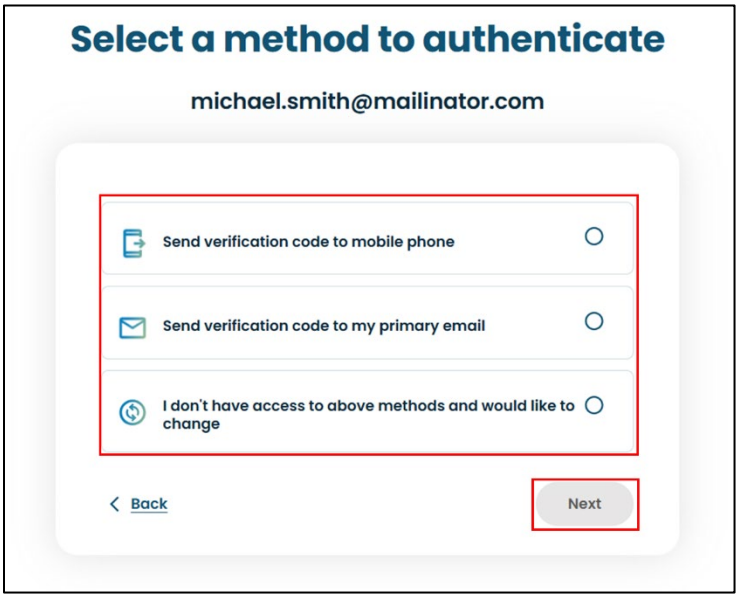
2. Removing MFA from an Existing Account

Removing Multi-Factor Authentication (MFA) allows you to regain access to your account if you need to reconfigure your security settings or if you lost access to your MFA option. By following the steps below, you can securely remove your MFA.

1. Login into the KYID platform with the help of your existing credential details. On the dashboard, select the **Username** drop down in the top right corner of the screen.
2. Select **My account** from the menu.

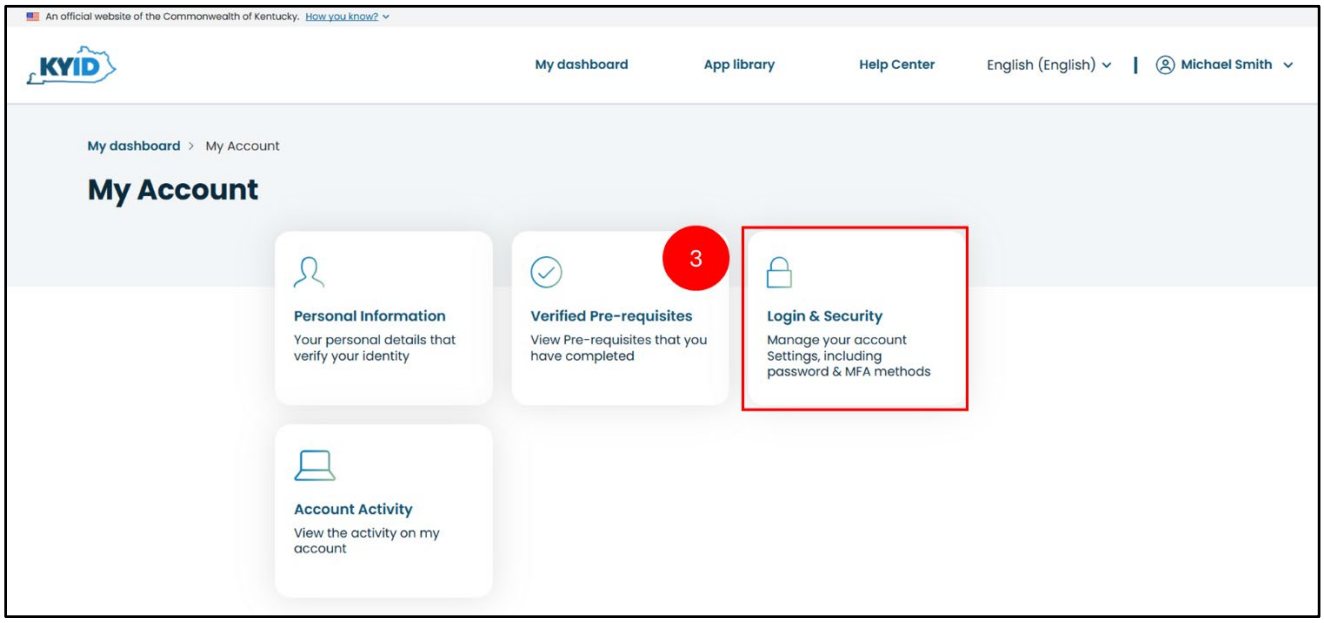


If this is your first time accessing the **My account** page, you are prompted to authenticate with either your mobile phone or through your primary email address tied to your KYID account. A verification code will be sent to either your mobile phone through text message or voice call or it will be sent to your primary email address. Select the option you desire and enter the verification code to continue.

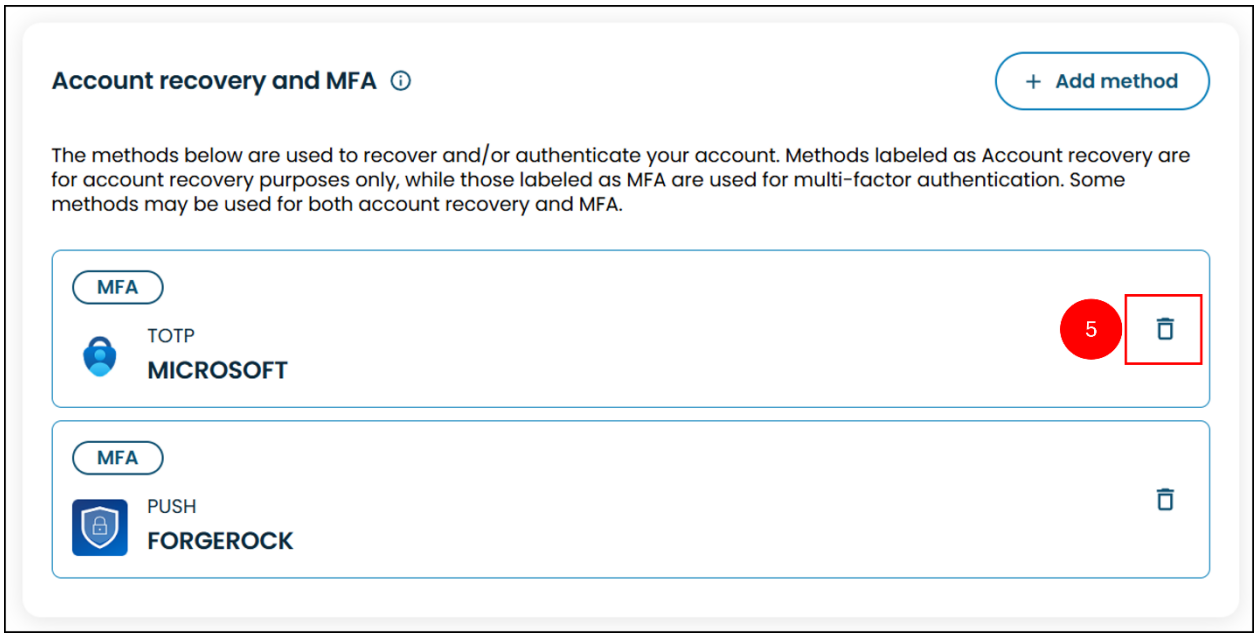


Please note: If you do not have access to the above methods and would like to change, you may verify your identity through Identity verification or by entering a verification code sent to your primary and alternate emails.

3. Click the **Login & Security** tile on the **My account** screen.



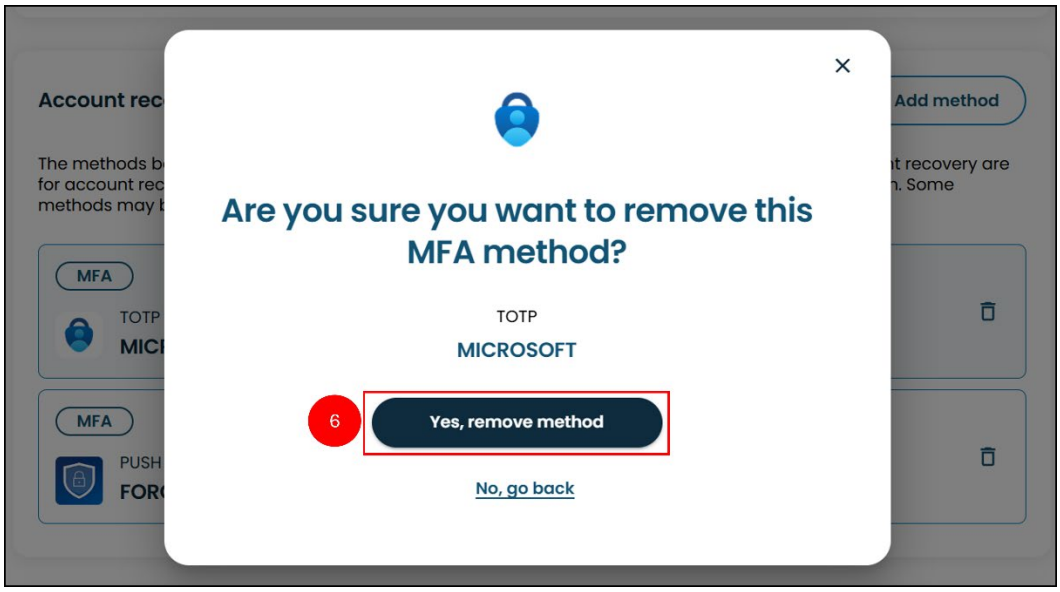
4. Scroll down to review the **Account recovery and MFA** tile on this screen.
5. Select the **trash** icon next to an MFA method you want to remove.



Please note: The **Account Recovery and MFA** section displays the methods available for recovering and authenticating your account. Methods labeled **Account Recovery** are used solely for account recovery, while those labeled **MFA** are used for multi-factor authentication. Some methods may serve both purposes.

You can add new methods or remove any methods labeled as **MFA** or **Account Recovery**, except for at least one **Account Recovery** method. It is mandatory to retain at least one method labeled **Account Recovery** to ensure you can recover your account if needed.

6. Select **Yes, remove method** on the **Are you sure you want to remove this MFA method** popup.



7. When the selected MFA method is removed successfully, a message will be displayed on the screen with the message: **You have successfully removed an MFA method**.