

The Commonwealth of Kentucky
kynect State-Based Marketplace



Agent Welcome Packet

Introduction

This Welcome Packet is designed to onboard and introduce new Agents to the Kentucky Health Benefit Exchange's systems and programs. This document provides an overview of the onboarding process and detailed onboarding steps. Additional Agent training materials can be found on the [KHBE website](#).

Table of Contents

Introduction..... 2

Table of Contents 2

1 Welcome Letter..... 3

2 Agent Onboarding Glossary of Terms..... 4

3 Creating a New KYID Account for Agents..... 6

 3.1 Steps to Create a New Agent KYID Account..... 6

 3.2 User Verification – Identity Proofing 18

 3.3 Kentucky Organ Donor Registration..... 22

4 Agents who Already Have KYID Accounts..... 24

 4.1 Obtaining COLT DHPO Training (Agent Training) Tile In KYID..... 24

 4.2 Accessing COLT and Completing Trainings..... 26

5 Multi-Factor Authentication 29

 5.1 Set up MFA: Via Authentication Applications 29

 5.2 Set up MFA: Mobile Number Authentication..... 48

 5.3 Add/Remove MFA Security Methods 51

6 Login Instructions..... 56

1 Welcome Letter

Getting Started with the Kentucky Health Benefit Exchange

Welcome to the Kentucky Health Benefit Exchange (KHBE) Program! KHBE oversees and manages the program, the certification/registration process, education and outreach, and program information for the State-Based Marketplace (SBM).

Agents use the SBM to enroll individuals and businesses in healthcare through the kynect Self-Service Portal (SSP). Agents use the SSP and Agent Portal to intake new clients, browse plans, generate reports, create proposals, and view all incoming notifications and announcements from Worker Portal.

KHBE coordinates and monitors the training requirements for Agents to access the SSP and Agent Portal. This packet outlines the necessary steps and requirements Agents must complete before they can access any KHBE trainings. As public health emergencies arise, these steps and requirements may be modified. If this does occur, the Agent will receive communications with specific updates and details. Agents must read the instructions carefully as they navigate through the process and follow the steps in the order they are listed. Do not skip any steps.

KHBE Team

2 Agent Onboarding Glossary of Terms

KHBE has put together a glossary of terms for Agents to review to help through the onboarding process.

Term	Definition
Advance Premium Tax Credit (APTC)	A tax credit Individuals can take in advance to lower their monthly health insurance payment (or “premium”). The advanced payment is reconciled on the year’s tax return. Based on the payment assistance the Individual qualifies for, their tax credit may change. This is also referred to as “Payment Assistance”.
Agent Training Role	A role assigned to Agents in the KYID that grants them access to training and QHP enrollment.
Commonwealth Offerings for Learning & Training (COLT)	The Commonwealth of Kentucky's Learning Management System (LMS) where kynectors and Agents complete training.
kynect	A Commonwealth of Kentucky website where individuals apply for benefit programs and resources including: Medicaid, Qualified Health Plan (QHP), Advance Premium Tax Credit (APTC), Kentucky Children's Health Insurance Program (KCHIP), Kentucky Integrated Health Insurance Premium Payment (KI-HIPP) Program, Supplemental Nutrition Assistance Program (SNAP), Kentucky Transitional Assistance Program (KTAP), and Child Care Assistance Program (CCAP). There are three systems that make up kynect: • kynect benefits • kynect resources • kynect health coverage
State-Based Marketplace (SBM)	State-owned marketplace through which consumers and small businesses can obtain health and/or dental insurance coverage.

Kentucky Children's Health Insurance Program (KCHIP)	A program that provides health coverage to children facing barriers such as high cost and lack of access to coverage. This applies to children under the age of 19.
KYID	Formerly known as the Kentucky Online Gateway (KOG). A website, KYID.ky.gov , that Agents visit to access the Agent Portal.
Medicaid	A federal and state program that provides health coverage to low-income adults, pregnant women, children, and individuals with disabilities.
Qualified Health Plan (QHP)	An insurance plan certified by the State-Based Marketplace that provides essential health benefits, follows established limits on cost-sharing (like deductibles, copayments, and out-of-pocket maximum amounts), and meets other requirements under the Affordable Care Act.

Please note: For an extended version of this glossary, go to the [KHBE Glossary for Agents and kynectors](#) on KHBE.ky.gov.

For more information on the benefit programs mentioned above, go to [kynect.ky.gov](https://www.kynect.ky.gov).

3 Creating a New KYID Account for Agents

To access the Agent training on COLT, Agents must create a KYID account. Follow the steps below to create a KYID account.

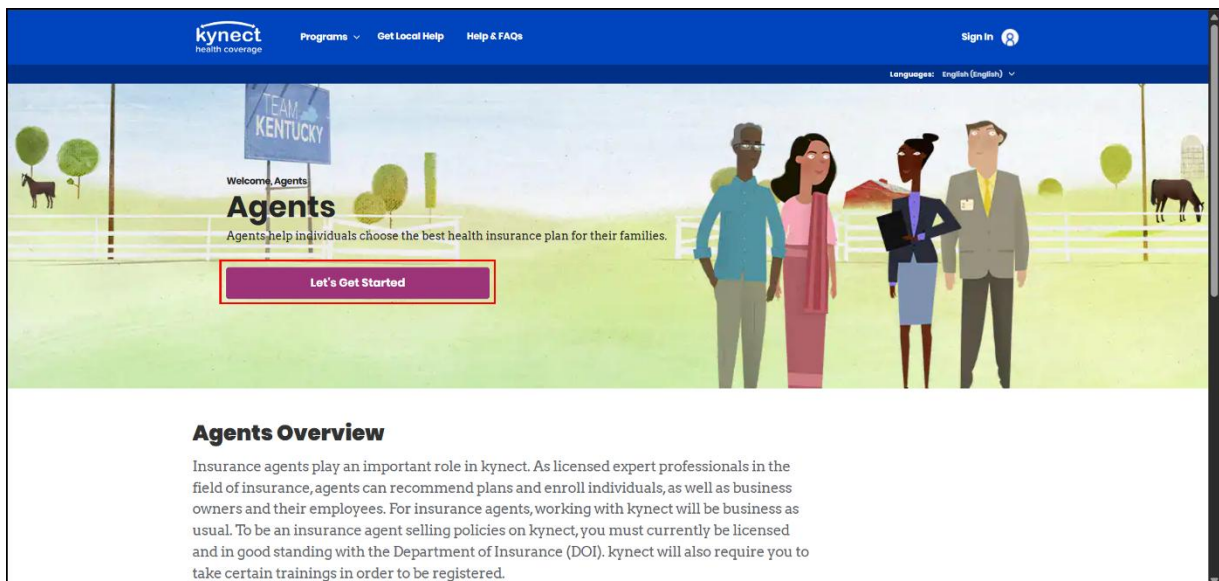
Please note: Individuals who already have a KYID account should NOT create a new account and should use their existing KYID account to access the trainings in COLT. If an Agent already has a KYID account, skip to [Section 6](#) of this document.

Please note: When creating a KYID account, Agents must enter their own information and create the account on behalf of themselves. For example, an Agent's assistant may not create a KYID account for them.

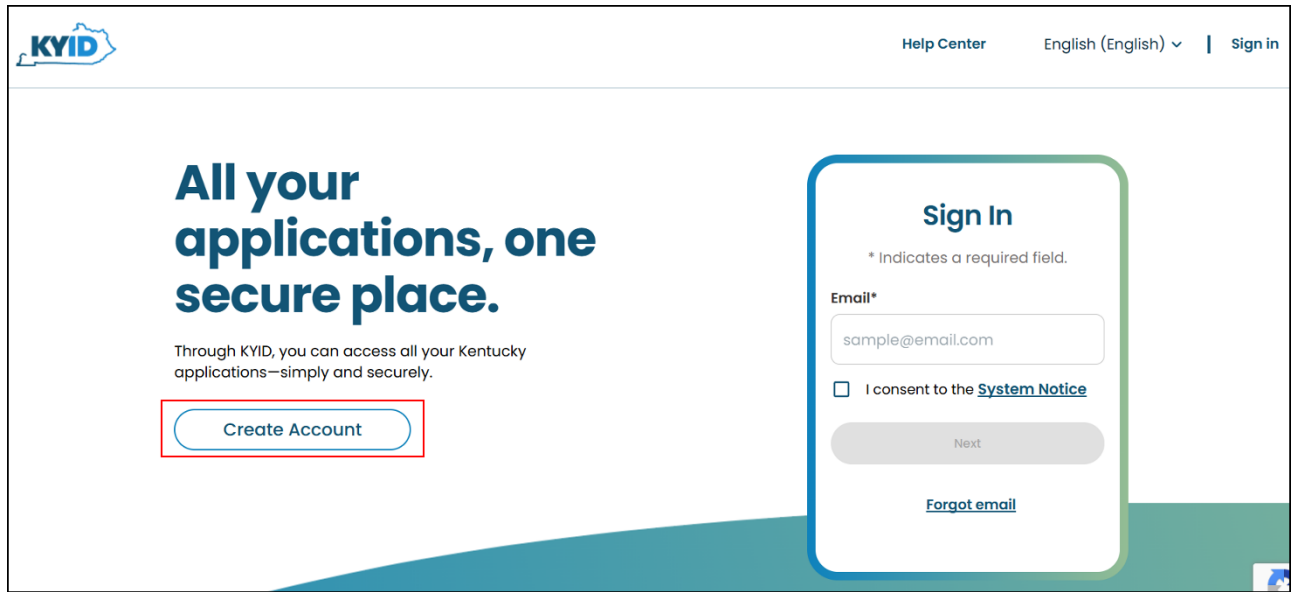
Please note: Agents must use their full legal first and last name matching their Insurance License when creating a KYID account. Do NOT use an assistant's name or a nickname when creating a KYID account.

3.1 Steps to Create a New Agent KYID Account

1. Navigate to the [KHBE Insurance Agents page](#).
2. Select **Let's Get Started** button.

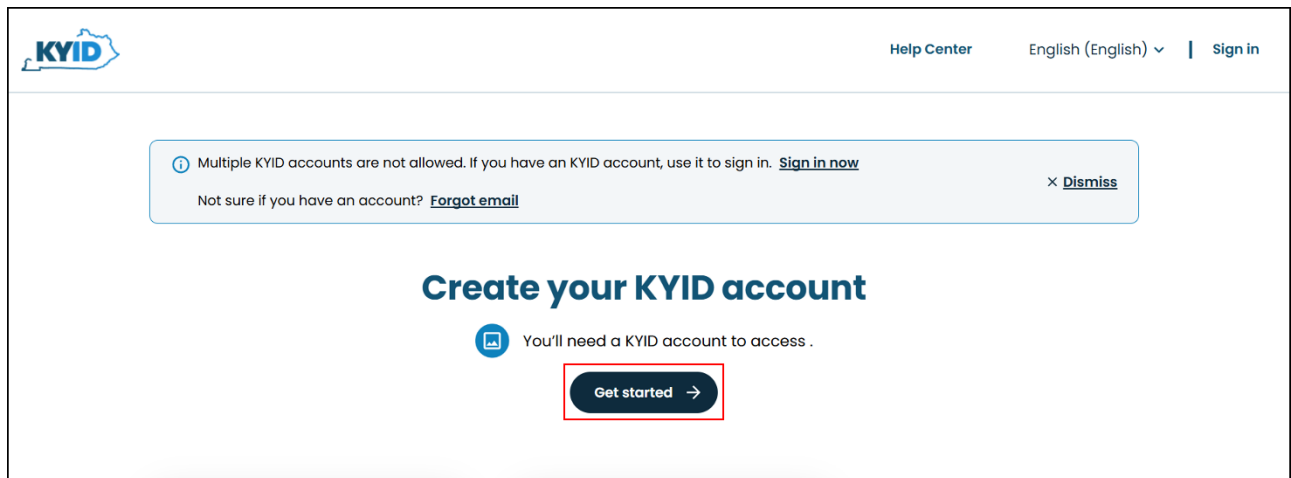


3. Select **Create New Account**.



The screenshot shows the KYID homepage. The header includes the KYID logo, a 'Help Center' link, a language dropdown set to 'English (English)', and a 'Sign in' link. The main content area features the heading 'All your applications, one secure place.' followed by a subtext: 'Through KYID, you can access all your Kentucky applications—simply and securely.' Below this, a 'Create Account' button is highlighted with a red rectangular box. To the right, there is a 'Sign In' section with a text input field for 'Email*' containing 'sample@email.com', a checkbox for 'I consent to the [System Notice](#)', a 'Next' button, and a '[Forgot email](#)' link.

4. Select **Get Started** on the KYID homepage.



The screenshot shows the 'Create your KYID account' screen. The header is identical to the previous page. A light blue notification banner at the top states: 'Multiple KYID accounts are not allowed. If you have an KYID account, use it to sign in. [Sign in now](#)' with a 'Dismiss' link. Below the banner, the heading 'Create your KYID account' is displayed. Underneath, a message says 'You'll need a KYID account to access .' with a key icon. At the bottom, a dark blue 'Get started →' button is highlighted with a red rectangular box.

Please note: The **Create your KYID Account** screen displays when you initiate the account creation process from the KYID home page. You may select the **Sign in** now link if you already have an account on the KYID portal. Select the **Forgot email** link in case you are not sure whether you already have an existing KYID account.

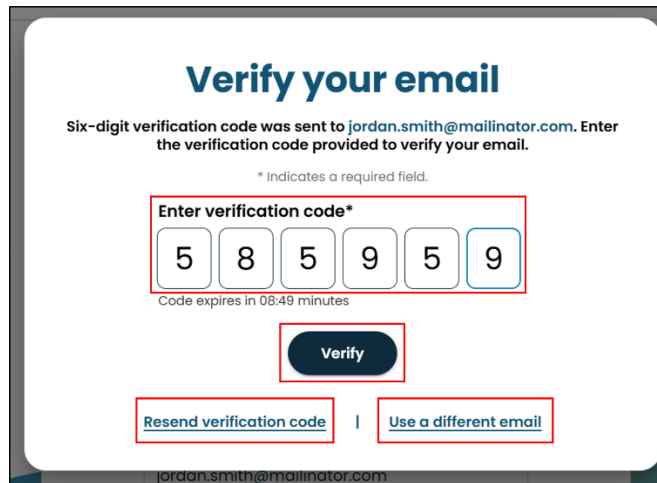
5. The **Enter your account email** is the first step of the account creation process. Enter your preferred **email address** in the *Primary email** field.
6. Enter the **same email id** in the *Confirm primary email** field.
7. Select **Next** to proceed.

The screenshot shows a web interface for creating an account. At the top, there's a link 'Exit create an account' and a progress indicator for 'Create an Account' showing 'Step 1 of 5'. The main heading is 'Enter your account email'. Below this, a message states 'Your email will serve as your username for your KYID account.' with a note '* Indicates a required field.' There are two input fields: 'Primary email*' and 'Confirm primary email*', both containing the email 'jordan.smith@mailinator.com'. At the bottom, there are two buttons: a '< Back' link and a 'Next' button.

Please note: You may select the **Back** link if you want to go to the previous screen. In case you want to exit this screen, select the **Exit create an account** link at the top left of

The **Verify your email** popup displays. As the next step in the account creation process, you must verify your email. A six-digit verification code is sent to your registered email address.

8. Enter the **six-digit code** in the *Enter verification code** field. Note that the code expires after **10** minutes.
9. After entering the code, select **Verify** to proceed. Upon successful verification, a success message is displayed.
10. Select the **Resend verification code** link to receive a new code in case the code expires after 10 minutes, or you have not received it.
11. Select the **Use a different email** link in case you wish to use a different email address to create your KYID account.



Verify your email

Six-digit verification code was sent to jordan.smith@mailinator.com. Enter the verification code provided to verify your email.

* Indicates a required field.

Enter verification code*

5 8 5 9 5 9

Code expires in 08:49 minutes

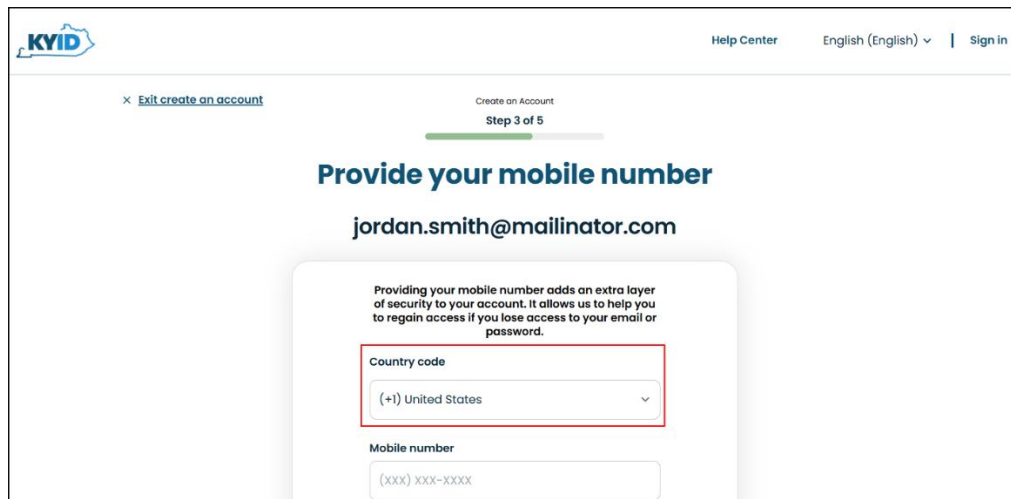
Verify

[Resend verification code](#) | [Use a different email](#)

jordan.smith@mailinator.com

The **Provide your mobile number** is the next step of the account creation process. You may select the **Skip this step** link on this screen, however, if you skip this step, then you must provide an alternate email as a mandatory step on the next screen. The mobile number or alternative email will be used for **Multifactor Authentication (MFA)** and/or for account recovery.

12. Select the **Country code** drop-down arrow and select the applicable country code from the menu.



KYID Help Center English (English) ▾ Sign in

[× Exit create an account](#)

Create an Account
Step 3 of 5

Provide your mobile number

jordan.smith@mailinator.com

Providing your mobile number adds an extra layer of security to your account. It allows us to help you to regain access if you lose access to your email or password.

Country code

(+1) United States ▾

Mobile number

(xxx) xxx-xxxx

13. Enter your mobile number in the *Mobile number* field.
14. Re-enter the same mobile number in the *Confirm mobile number* field.
15. 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.
16. Select **Next** to proceed.

The screenshot shows a mobile number verification form. At the top, there is a 'Country code' dropdown menu with '(+1) United States' selected. Below this are two input fields: 'Mobile number' and 'Confirm mobile number', both containing '(859) 555-1234'. These two fields are highlighted with a red rectangular box. Below the input fields is a section titled 'How would you like to receive the verification code?'. It contains two radio button options: 'Text Message' (which is selected, indicated by a blue checkmark) and 'Voice call'. The 'Text Message' option includes a text icon and the description 'You will receive a passcode via text message to your phone'. The 'Voice call' option includes a phone icon and the description 'You will receive a passcode via voice call to your phone'. Below these options is a small disclaimer: 'By providing your mobile phone number you are consenting to receive messages (Standard data rates may apply)'. At the bottom of the form, there is a link 'Skip this step' and two buttons: a 'Back' button with a left arrow and a 'Next' button, which is highlighted with a red rectangular box.

The **Verify your mobile number** popup displays. As the next step in the account creation process, you must verify your mobile number. A **six-digit verification code** is sent to the mobile number you provided.

17. Enter the six-digit code in the *Enter verification code** field. Note that the code expires after 5 minutes. You must enter the code before it expires.
18. After entering the code, select **Verify** to proceed. Upon successful verification, a success message appears.

If you need a new code sent to your mobile device:

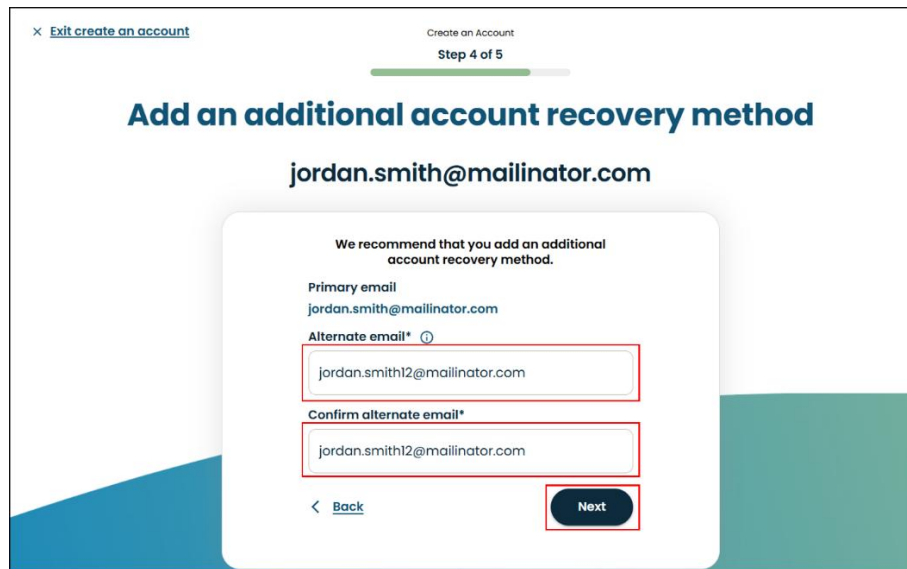
- Select the **text message** link to receive a new code via text message in case the code expires, or you have not received it.
- Select the **voice call** link in case you prefer to receive the code via a voice call.

Please note: The retry limit is **three (3)**, for resending verification code through text message or voice call; that includes one primary and two retries. If you provide an incorrect verification code for the third time, an error message will be displayed.

You may select the **Back** link to go back to the previous screen.

The **Add an additional account recovery method** is the next step in the account creation process. This step is optional if you have already provided your phone number. However, if you skipped the step to enter your phone number earlier, this step becomes mandatory. Confirm that your **Primary email** is displayed correctly on this screen.

19. Enter your alternate email address in the *Alternate email** field.
20. Re-enter the alternate email address in the *Confirm Alternate email** field and confirm it matches the one entered above.
21. Select **Next** to proceed.



The screenshot shows a web interface for creating an account, specifically Step 4 of 5. The title is "Add an additional account recovery method". Below the title, the primary email "jordan.smith@mailinator.com" is displayed. A message states: "We recommend that you add an additional account recovery method." The form contains three fields: "Primary email" (jordan.smith@mailinator.com), "Alternate email*" (jordan.smith12@mailinator.com), and "Confirm alternate email*" (jordan.smith12@mailinator.com). The "Alternate email*" and "Confirm alternate email*" fields are highlighted with red borders. At the bottom, there are "Back" and "Next" buttons. The "Next" button is highlighted with a red border.

Please note: Other mandatory MFA options may be prompted based on your user role. Please refer to the [Manage MFA User Guide](#) for detailed instructions on setting up the available MFA options.

22. The **Verify your email** popup displays. Enter the code sent to the alternate email, in the *Enter verification code** field, and then select **Verify**.

The screenshot shows a 'Create an Account' window at 'Step 4 of 5'. A modal titled 'Verify your email' is displayed. It states: 'Six-digit verification code was sent to jordan.smith12@mailinator.com. Enter the verification code provided to verify your email.' Below this, a note says '* Indicates a required field.' The input field is labeled 'Enter verification code*' and contains the digits 5, 0, 8, 5, 9, 0. A timer below the field indicates 'Code expires in 09:22 minutes'. A 'Verify' button is positioned below the input field. At the bottom of the modal are two links: 'Resend verification code' and 'Use a different email'. The background shows a 'Next' button and a 'Back' link.

The **Enter your personal information** is the next step of the account creation process. This step enables you to add or update your personal information details like basic information, home details, and contact information.

23. Under the **Basic information** section, enter relevant data in the following fields.

The screenshot shows the 'Basic information' section of a form. It includes a note: 'Please ensure that you have entered the following information correctly to ensure a seamless and secure process.' followed by a bulleted list: 'Full legal name', 'Gender', 'Date of birth', and 'Current home address'. Below this, it says: 'You have higher chances of successfully completing the identity verification if you provide social security number.' A red box highlights the following fields: 'Legal first name*', 'Legal middle name', 'Legal last name*', 'Suffix', 'Gender', 'Date of birth*' (with a calendar icon), and 'Social Security Number (SSN) / Individual Taxpayer Identification Number (ITIN)' (with a mask 'XXX-XX-XXXX' and a search icon). A note '*Indicates a required field.' is located above the first name field.

☐ I don't have a home address

Address 1*	Address 2
City*	State*
	Kentucky
Zip/postal code*	Zip/postal code extension
Country*	County
United States	

Identity verification is limited to US addresses and US territories only.

[< Back](#) [Next](#)

Please note: If the system is unable to confirm your address with the USPS, you will encounter a pop-up alerting you to check that you entered your address correctly.

The **Create a password** is the final step of the account creation process. Review the password requirements which meet the specified policy rules, which are indicated at the top of the form.

24. Enter your desired password in the **Password*** field ensuring it meets the strength requirements.
25. Re-enter the password in the **Confirm password*** field. If the passwords do not match, then the **Create Account** button will remain disabled.
26. Select **Create account** to finalize the account setup.

The screenshot shows a mobile app interface for creating a password. At the top, a section titled "Passwords must meet the following:" lists six requirements, each with a green checkmark: "Have at least 8 characters", "Should not contain the first name or last name", "Have at least one lowercase letter", "Have at least one uppercase letter", "Have at least one numeric digit", and "Should contain special characters". Below this list is a small note: "* Indicates a required field." The "Primary email" field is populated with "jordan.smith@mailinator.com". There are two password input fields: "Password*" and "Confirm password*", both with red borders and masked with dots. The "Confirm password*" field has a "Very Strong" strength indicator above it. At the bottom left is a "< Back" link, and at the bottom right is a "Create account →" button with a red border.

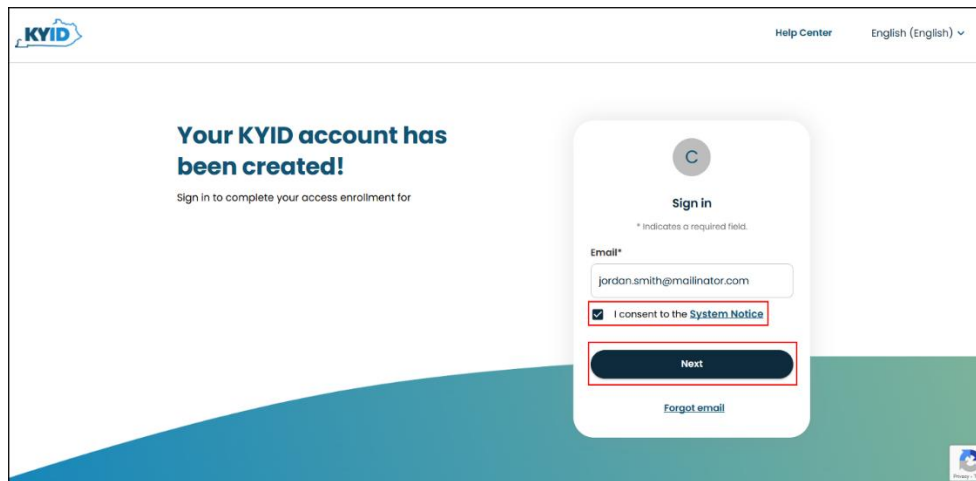
Please note: The new password:

- must have at least 8 characters,
- should not contain the first name or last name,
- must have at least one lowercase letter,
- must have at least one uppercase letter,
- must have at least one numeric digit, and
- should contain special characters.

If all the above criteria for a strong password are met, then the Create Account button will be enabled.

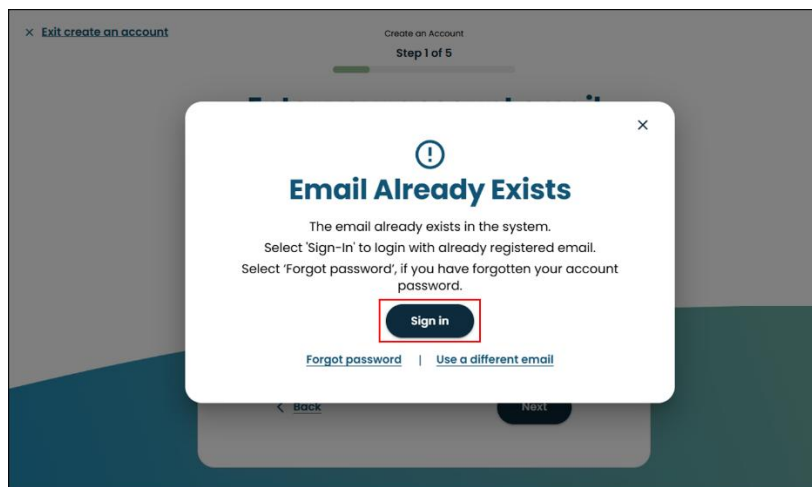
A confirmation message is displayed stating that your KYID account has been created. To complete your registration, sign-in to the KYID portal with the new credentials. The email ID is auto populated in the *Email** field.

27. Select the **I consent to the System Notice** checkbox.
28. Select **Next** to proceed.



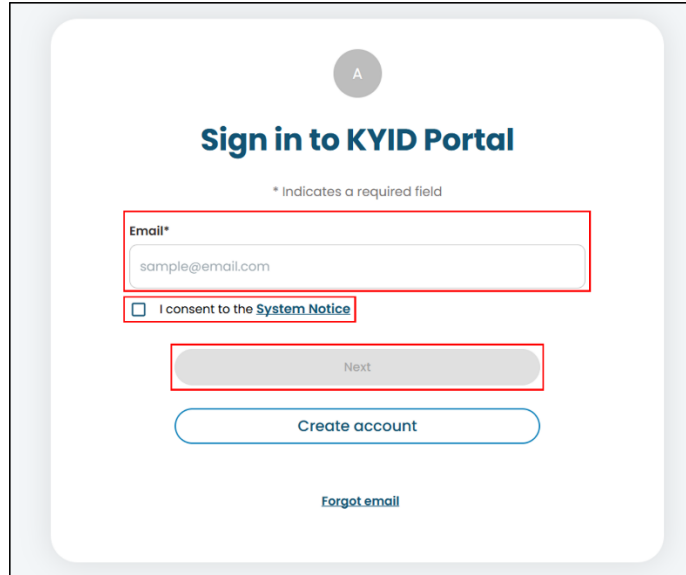
While creating your KYID account, if the email provided as the primary email address is already registered on the KYID portal, then the **Email Already Exists** popup displays.

29. Select **Sign in** to log in with your already registered email.



Please note: You may select the **Forgot password** link to initiate the password recovery process, in case you have forgotten the password, or you may select the **Use a different email** link in case you prefer to use a different email address to sign in.

30. Enter your registered email address in the *Email** field.
31. Select the **I consent to the System Notice** checkbox.
32. Select **Next** to proceed.



The screenshot shows a sign-in form for the KYID Portal. At the top, there is a circular logo with the letter 'A'. Below the logo, the title 'Sign in to KYID Portal' is displayed. A small asterisk note indicates that fields marked with an asterisk are required. The form contains an 'Email*' input field with the placeholder text 'sample@email.com'. Below this is a checkbox labeled 'I consent to the System Notice'. A 'Next' button is positioned below the checkbox, and a 'Create account' button is located further down. At the bottom of the form, there is a link for 'Forgot email'.

Please note: Once you have entered the email address and have selected the consent notice checkbox, then the **Next** button will be enabled.

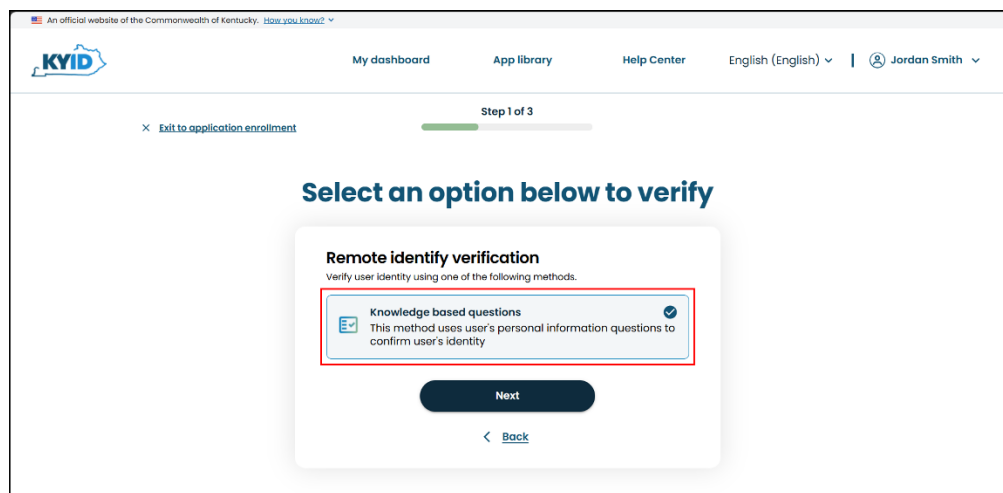
You may select **Create account** button to create a new account, or you may select the **Forgot email** link to recover your account.

3.2 User Verification – Identity Proofing

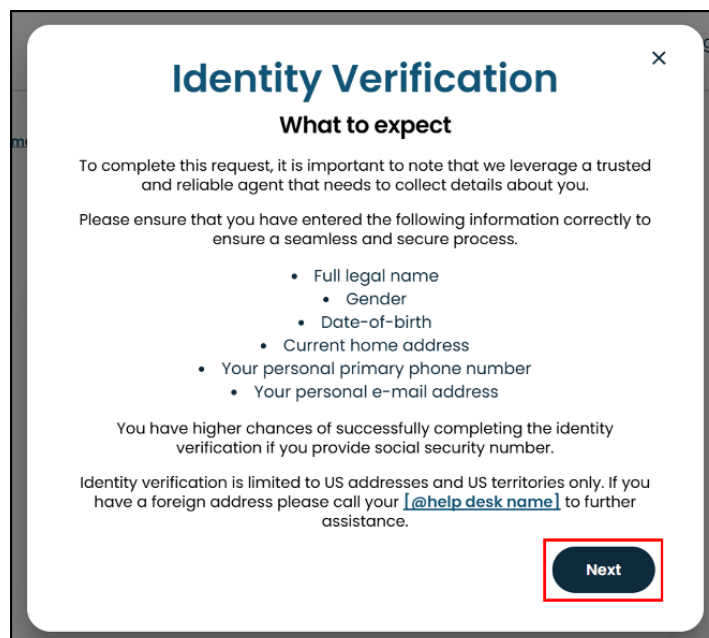
KYID uses Remote Identity Proofing (RIDP) to verify the user's identity. This is a one-time effort. If a user is requesting electronic access to protected information or systems, the user must be identity proofed to gain access. KYID uses the Experian identity verification system to remotely perform identity proofing.

KYID uses this personal information only to verify the user's identity. Experian verifies the information provided against their records and may present the user with questions based on their credit profile. KYID does not store this information. This type of inquiry, a soft inquiry, does not affect your credit score.

1. Select **Knowledge based questions** option on the **Select an option below to verify** screen, and then select **Next**.



2. Read the instructions on the **What to expect** popup, then select **Next**.



3. Provide and review answers to each required question marked with an asterisk (*). Select **Next**.

Basic information

Please ensure that you have entered the following information correctly to ensure a seamless and secure process.

- Full legal name
- Gender
- Date of birth
- Current home address

You have higher chances of successfully completing the identity verification if you provide social security number.

*Indicates a required field.

Legal first name*	Legal middle name
Legal last name*	Suffix
Gender	Date of birth* ⓘ
	Month Name, Date, Year

Social Security Number (SSN) / Individual Taxpayer Identification Number (ITIN)

Home address

☒ I don't have a home address

Address 1

Address 2

City*

State*

Zip/postal code

Zip/postal code extension

County

Country

Contact

Primary email*

Mobile Number

By checking this box, I certify that I understand that, in requesting these services, my identity may be verified through other sources. Any information collected by the Cabinet for Health and Family Services (CHFS) may be used to verify my identity in accordance with 15 U.S.C. § 1681b(a)(3)(D). I understand that my information will be used solely to verify my identity and to prevent fraudulent transactions in connection with my request to create an account to access public services or benefits.

To prevent fraud and verify my identity or my wireless device, I authorize my wireless carrier to use or disclose information about my account and wireless device, if available, to CHFS or its service provider for the duration of my business relationship. See the [CHFS Privacy Policy](#) for details on how your data is treated.

☐ I have read, understand, and agree to the above terms and conditions

[< Back](#)
[Next](#)

Please note: If the system is unable to confirm your address with the USPS, you will encounter a pop-up alerting you to check that you entered your address correctly.

4. Experian verified the information provided and may present the user with questions based on their credit profile. Provide answers to each question. Select **Next**.

The screenshot shows the KYID application enrollment process at Step 3 of 3. The page title is "Answer a few questions". A disclaimer states: "Your information will be used for verification purposes only." The questionnaire consists of three questions, each with radio button options:

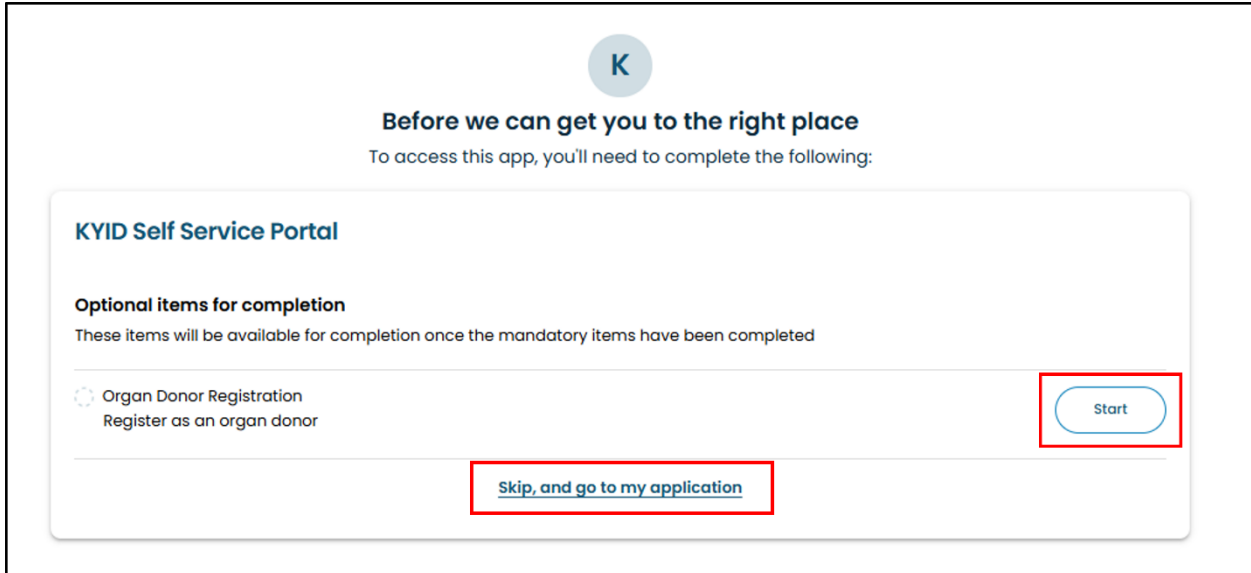
- What model car do you drive?
 - ☐ Ford
 - ☐ Chevy
 - ☐ Honda
 - ☐ Toyota
 - ☐ None of the above
- What is the year of your vehicle?
 - ☒ 2003
 - ☐ 2005
 - ☐ 2009
 - ☐ 2013
 - ☐ None of the above
- What is the name of the city where you previously lived?
 - ☒ Richmond
 - ☐ Little Rock
 - ☐ Spokane
 - ☐ Seattle
 - ☐ None of the above

At the bottom of the form, there is a "< Back" link and a "Next" button.

Please note: If the user does not have a credit history or Experian cannot perform identity proofing online, the user will be given a reference number and will need to call the Experian Help Desk. Please call the Experian Help Desk at 1-866-578-5409 and provide the reference number.

3.3 Kentucky Organ Donor Registration

When the user first logs into KYID, they will be prompted to register as an organ donor. To register as an organ donor, select **Yes, Register Now** and follow the prompts. If the user selects **Remind Me Later**, the system redirects to the KYID Dashboard.



The screenshot displays the KYID Self Service Portal interface. At the top, a blue circle with the letter 'K' is centered. Below it, the text reads: "Before we can get you to the right place" and "To access this app, you'll need to complete the following:". A white box with a light blue border contains the following elements: the title "KYID Self Service Portal", the section header "Optional items for completion", and a subtext "These items will be available for completion once the mandatory items have been completed". Below this, there is a list item: "Organ Donor Registration" with a subtext "Register as an organ donor". To the right of this item is a blue button labeled "Start". Below the list item is a blue link labeled "Skip, and go to my application".

If the user selects **Yes, I would like to register as an organ donor** the system navigates to the **Organ Donor Registration** screen where the user verifies their personal information. To complete registration, select the check box **I have read, understand, and agree to the above terms and conditions** and then select **Register**. The system redirects the user to the KYID Dashboard.

If at any point the user chooses to skip the organ donor registration process, select **Cancel** to navigate to the KYID Dashboard. You may register to be an Organ Donor at a later time.

Register as an organ donar

Organ donor registration

With the passing of KY SB77 and in partnership with Donate Life Kentucky, the Kentucky Online Gateway has created the below form for Kentuckians to join the Kentucky Organ Donor Registry. If you'd like to join the KYDR, please fill out the required fields below, select the consent checkbox, and click the "Register" button. For more information on what it means to be an organ donor <https://donatelifeky.org/why-donate/>

Basic information

* Indicates a required field.

The following information reflects your personal profile as maintained in our system. Any changes made below will be reflected in your personal profile once verification is successful

Legal first name*	Legal middle name
John	S
Legal last name*	Suffix
Smith	
Gender*	Date of birth*
Male	August, 14, 1991
Social security number	
XXX-XX-XXXX	

Address 1*	Address 2
City*	State*
	Kentucky
Zip code*	Zip extension
County*	
Drivers License or State ID*	

Contact

Primary email*	Mobile Number*
RMcClellan24@yopmail.com	XXX-XXX-XXXX

By checking this box, I certify that I understand that, in requesting these services, my identity may be verified through other sources. Any information collected by the Cabinet for Health and Family Services (CHFS) may be used to verify my identity in accordance with 15 U.S.C. § 1681b(a)(3)(D). I understand that my information will be used solely to verify my identity and to prevent fraudulent transactions in connection with my request to create an account to access public services or benefits.

To prevent fraud and verify my identity or my wireless device, I authorize my wireless carrier to use or disclose information about my account and wireless device, if available, to CHFS or its service provider for the duration of my business relationship. See the [CHFS Privacy Policy](#) for details on how your data is treated.

☒ I have read, understand, and agree to the above terms and conditions

[Cancel](#)

[Register](#)

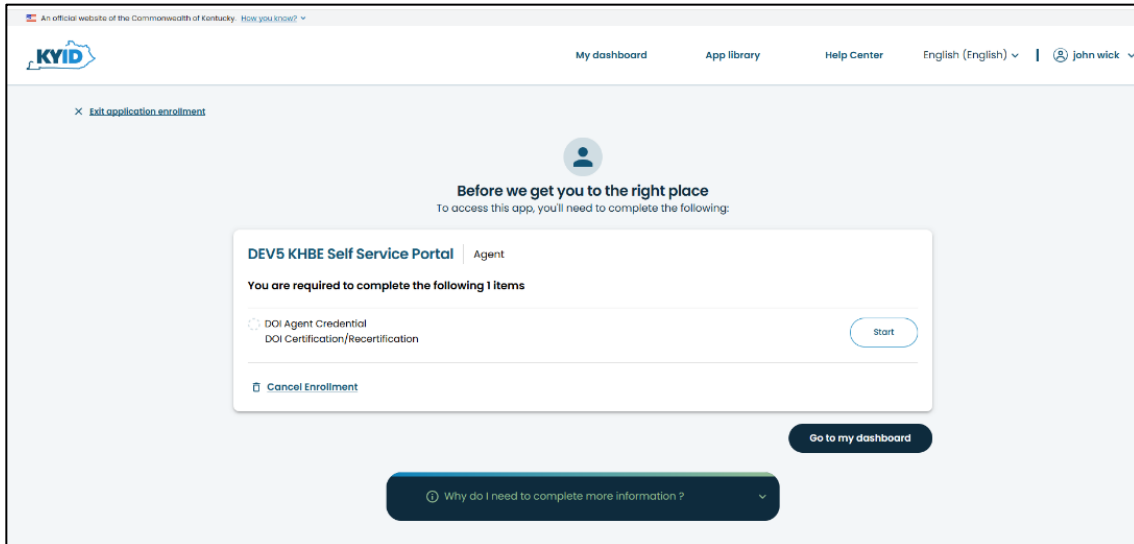
4 Agents who Already Have KYID Accounts

Individuals who already have a KYID account should NOT create a new account and should use their existing KYID account to access the trainings in COLT. The high-level process an Agent with an existing KYID account must complete is as follows:

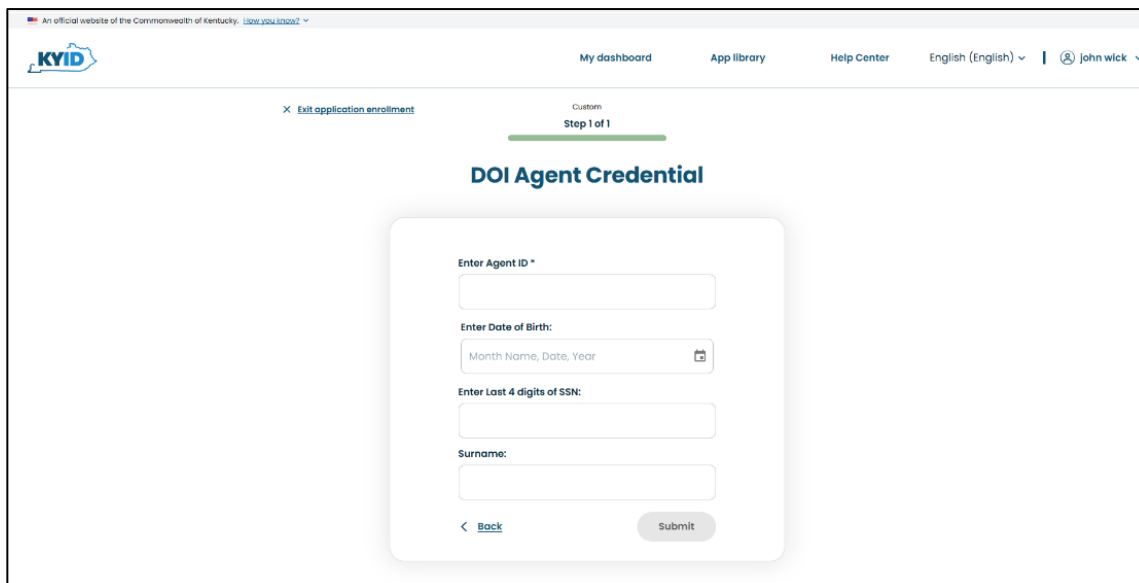
- **Obtaining COLT DHPO Training (Agent Training) Tile in KYID** - Navigate to the [kynect Insurance Agents page](#), select **Let's Get Started**, and log into your existing KYID account. Enter Agent information, navigate to the KYID homepage, and select **Launch** next to *COLT DHPO Training* tile in KYID.
- **Accessing COLT and Completing Trainings** - After signing into the COLT LMS, Agents will see their Dashboard display. Agents can select a course from the *Your Enrolled Training* section to begin training or enroll in additional courses through the *DHPO Training Catalog* section. Utilize the Search Bar to search for applicable training courses and content if needed.
- **Accessing Agent Portal** - After the Agent completes the State-Based Marketplace Training on COLT and passes the assessment, they may access the Agent Portal from the KYID homepage.

4.1 Obtaining COLT DHPO Training (Agent Training) Tile In KYID

1. Navigate to the [kynect Insurance Agents page](#) and select **Let's Get Started**.
2. Log into existing KYID account.
3. At this point, some users may be prompted to verify their identities. In this case, the Agent must provide answers to each required question to complete the Remote Identity Proofing (RIDP) process.
4. Enter in **Agent ID**. Enter any remaining details that are available and make sure all information is accurately entered on the Access Request screen. Then, select **Next**.
 - Your Agent ID is your Kentucky DOI number.
 - Do not enter your National Producer Number (NPN).
 - If you are unsure of your DOI number you may search for it [here](#).



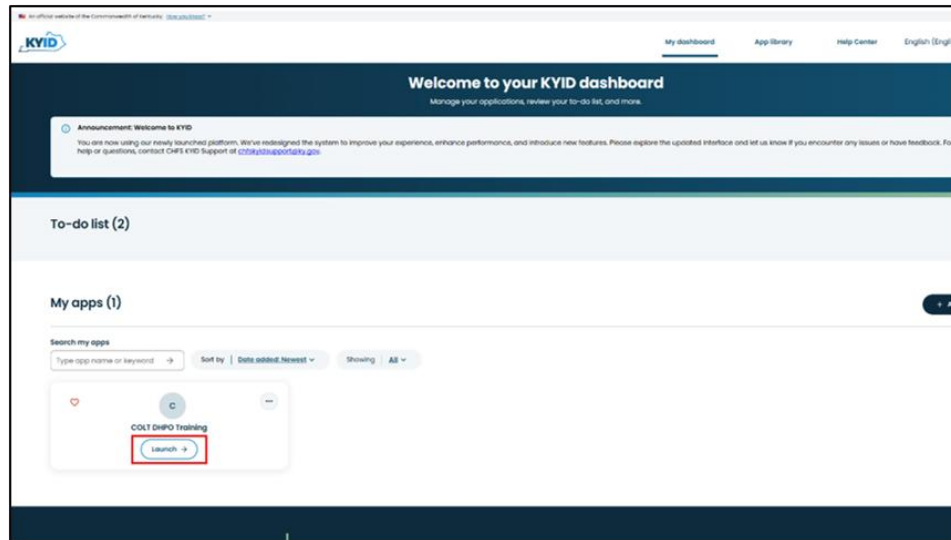
This screenshot shows the KYID Agent Welcome Screen. At the top, there is a navigation bar with the KYID logo, a link to 'How you know?', and user information for 'john wick'. Below the navigation bar, there is a central card titled 'Before we get you to the right place' with a sub-header 'To access this app, you'll need to complete the following:'. The card lists 'DEV5 KHBE Self Service Portal' as the selected option and 'Agent' as the role. It states 'You are required to complete the following 1 items' and lists 'DOI Agent Credential DOI Certification/Recertification'. There is a 'Start' button next to this item and a 'Cancel Enrollment' link at the bottom left of the card. A 'Go to my dashboard' button is located at the bottom right of the card. At the very bottom, there is a dark blue button with a question mark icon and the text 'Why do I need to complete more information?'.



This screenshot shows the KYID DOI Agent Credential Setup Screen. The top navigation bar is identical to the previous screen. Below the navigation bar, there is a progress indicator showing 'Custom Step 1 of 1'. The main heading is 'DOI Agent Credential'. Below this, there is a form with the following fields: 'Enter Agent ID *' (text input), 'Enter Date of Birth:' (calendar icon), 'Enter Last 4 digits of SSN:' (text input), and 'Surname:' (text input). At the bottom of the form, there is a '< Back' link and a 'Submit' button.

Please note: Only one KYID account can be associated with an Agent ID.

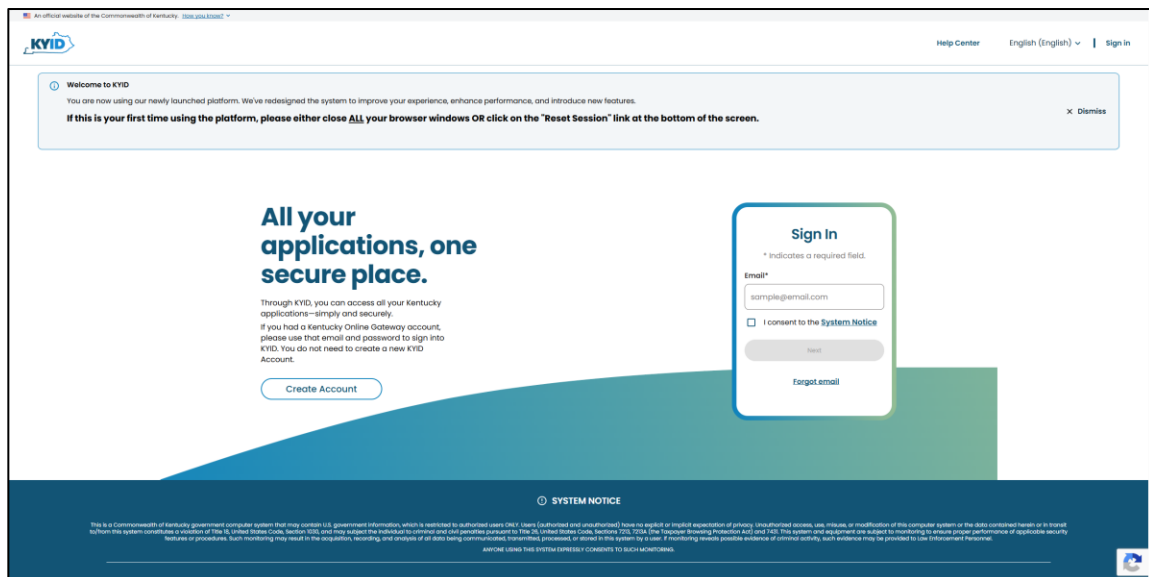
- Now, the Agent is prompted to set-up their multi-factor authentication (MFA). Follow the instructions in [Section 5](#) of this document to complete this process.
- After completing the MFA setup steps in [Section 5.1](#) of this document, navigate to the [KYID Homepage](#).
- Log into KYID using Agent KYID credentials.
- Navigate to the *COLT DHPO Training* tile and select **Launch**.



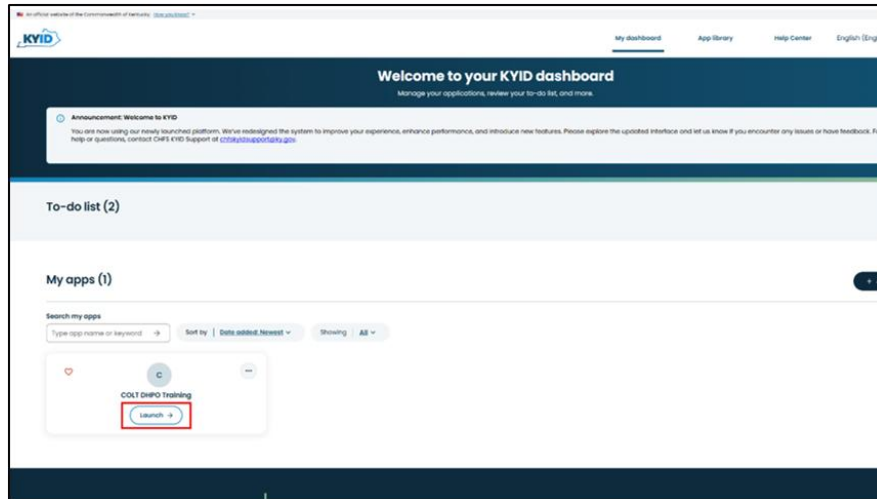
4.2 Accessing COLT and Completing Trainings

Agents must complete the State-Based Marketplace (SBM) Certification/Registration Training through COLT. Agents should follow the steps below to complete the SBM Certification/Registration Training annually.

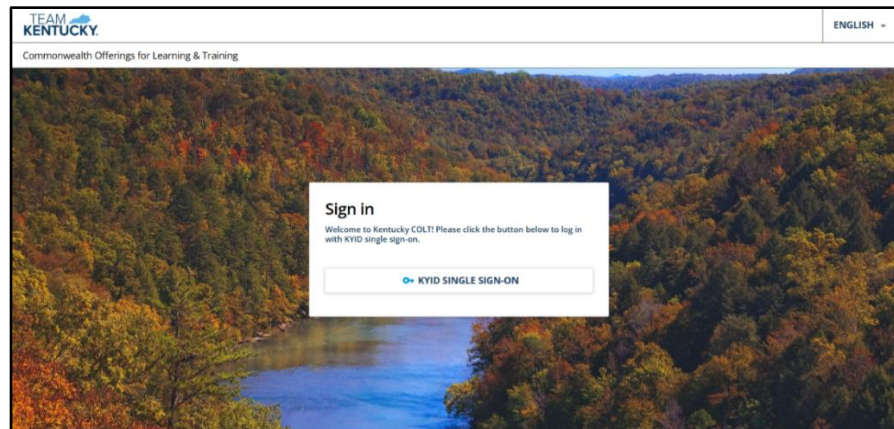
1. Navigate to the [KYID home screen](#).
2. Log into KYID using KYID credentials.



3. Navigate to the *COLT DHPO Training* tile from the KYID dashboard.
4. Select **Launch**.

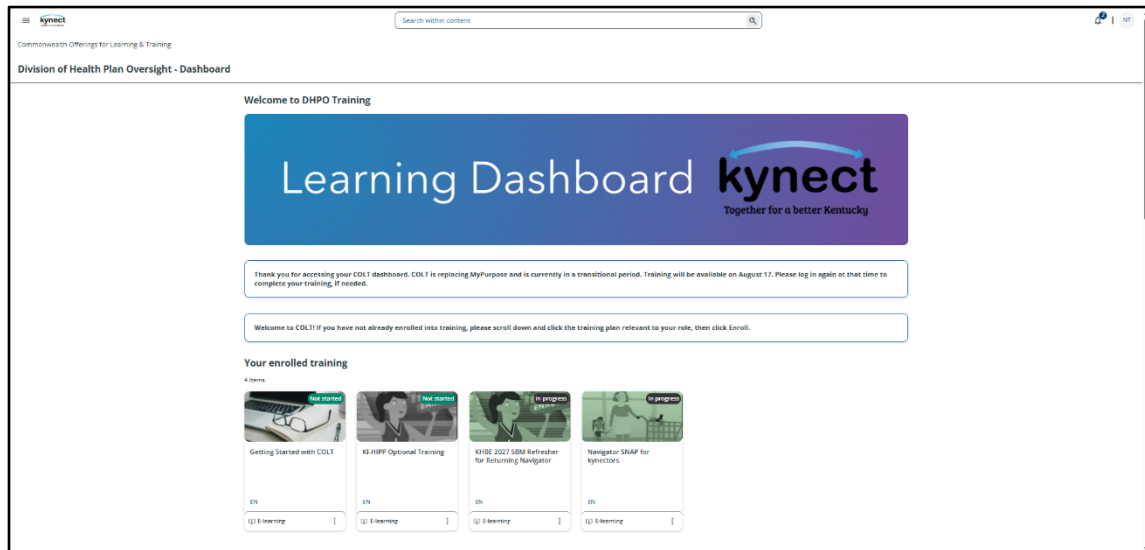


5. On the COLT LMS Sign In screen, select **KYID Single Sign-On** to navigate to your COLT LMS Dashboard.



After signing into the COLT LMS, Agents will see their Dashboard display. Agents can select a course from the *Your Enrolled Training* section to begin training or enroll in additional courses through the *DHPO Training Catalog* section. Utilize the *Search Bar* to search for applicable training courses and content if needed.

6. Under the *Your Enrolled Training* section, select the applicable **Course** then select **Start Learning Now** to begin training.
7. After completing all lessons of the required training, take the corresponding **Assessment**.



Please note: Agents are allowed 3 attempts to complete the assessment and must obtain a passing score of 80% or greater.

5 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an authentication method that requires Agents to provide two or more verification factors to gain access to COLT and kynect. Users may be presented with different security methods to complete MFA. Available MFA options include:

- ForgeRock
- Microsoft
- Google
- Symantec VIP
- Mobile phone

5.1 Set up MFA: Via Authentication Applications

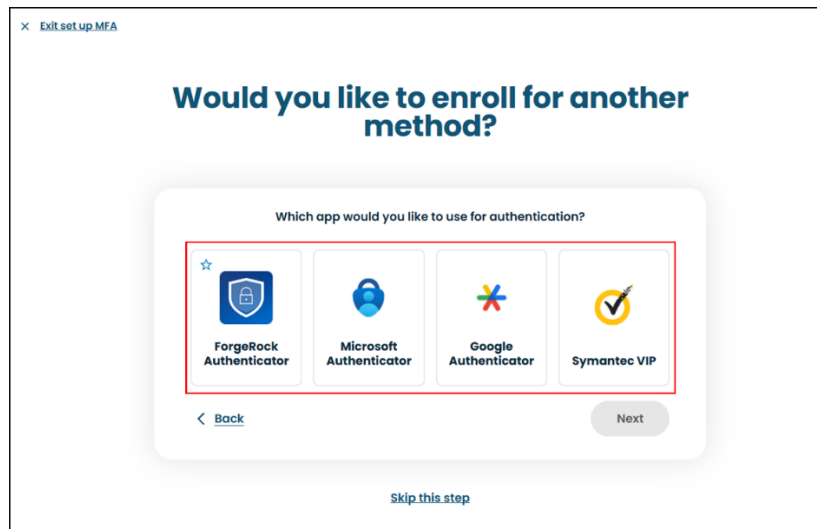
When logging into KYID for the first time, if the email address and password entered on the KYID login screen are correct, users will be asked to set up their multi-factor authentication. You have the option of choosing between:

Follow the steps below to setup one of the available authenticator applications.

1. Select the **Authentication Application** checkbox.
2. Select **Next** to proceed.

The screenshot shows a web interface for selecting an MFA method. At the top left, there is a link "Exit set up MFA". The main heading is "Select a multi-factor authentication (MFA) method". Below this, a question asks "How would you like to authenticate when signing into your account?". A note states "* Indicates a required field." There are two options: "Authenticator application" (which is selected with a checkmark and highlighted by a red box) and "Mobile phone". The "Authenticator application" option includes the instruction "Download and set up an application on your device to authenticate at sign in". At the bottom, there is a "Back" link and a "Next" button (highlighted by a red box).

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 these applications. If you prefer not to enroll in an additional MFA method, you can select the **Skip this step** link. Selecting this option will close the MFA setup window and redirect you to the **Login & Security** screen.



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.

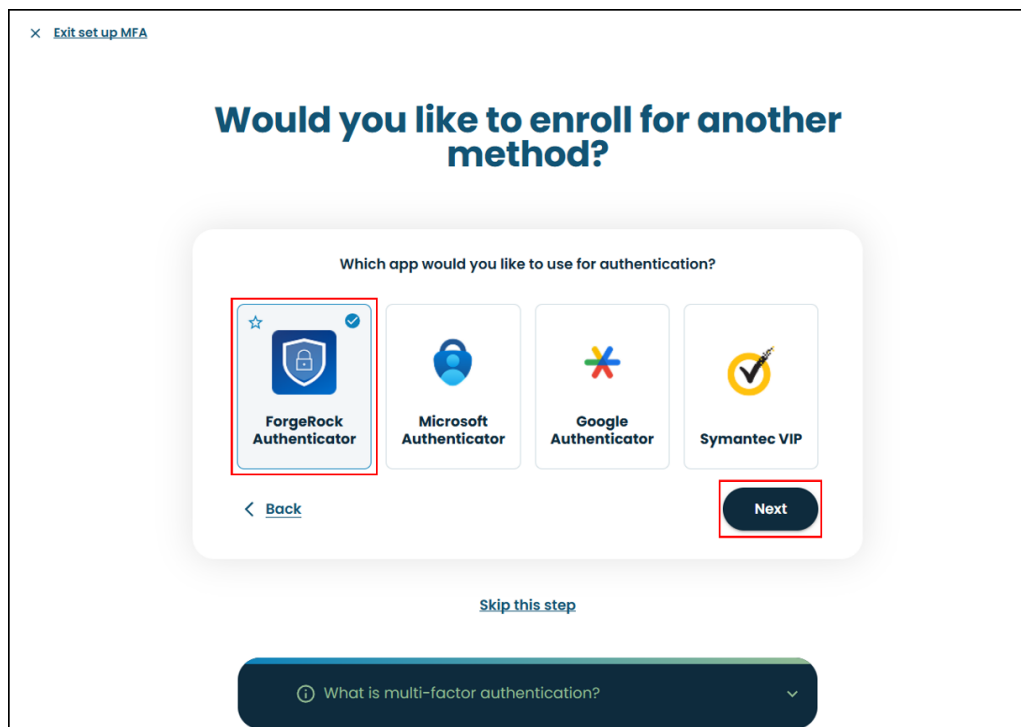
Prerequisites: Before you begin, confirm you have access to your primary email, and a mobile device with one of the following authenticator apps installed:

- Symantec VIP
- ForgeRock
- Google Authenticator
- Microsoft Authenticator

5.1.1 ForgeRock Authenticator Application

The **ForgeRock Authentication** 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 Authentication 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.

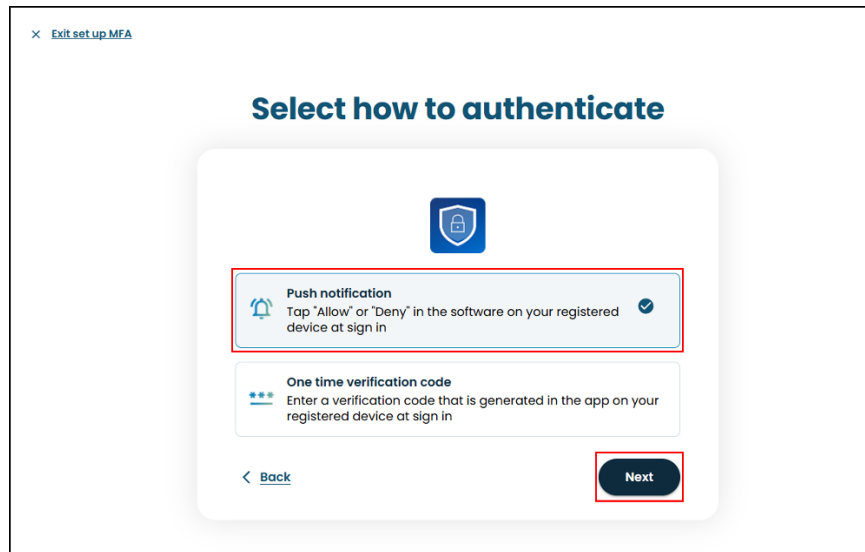
1. Select **ForgeRock Authenticator** on the **Would you like to enroll for another method?** screen.
2. Select **Next** to proceed.



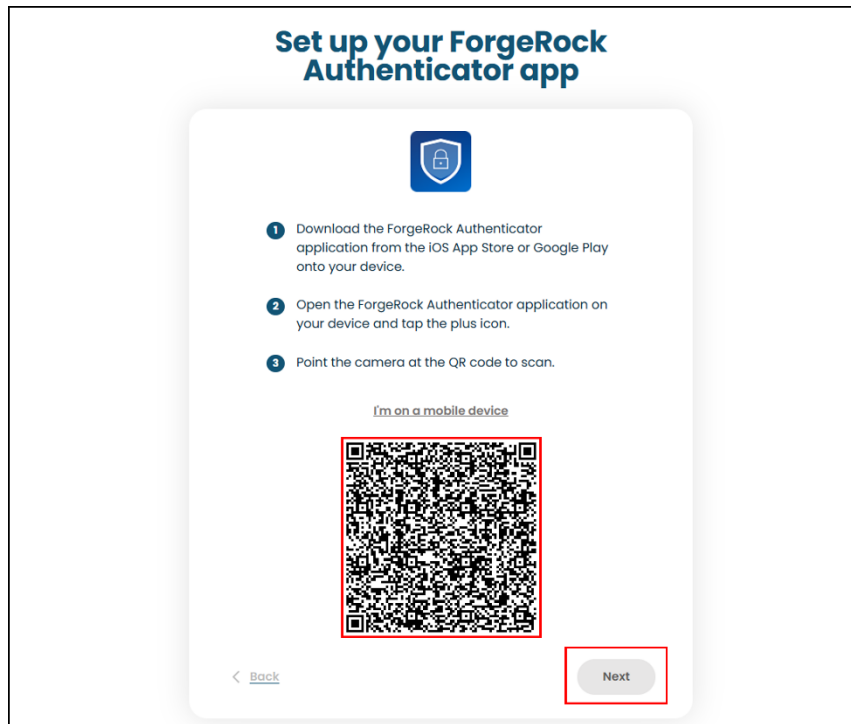
On the **Select how to authenticate** screen, two checkboxes are available **Push notification** checkbox or the **One time verification code**. **Push notification** checkbox can be selected to receive a notification on the mobile device with the options **Allow** or **Deny**. You can select **Allow** 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**.

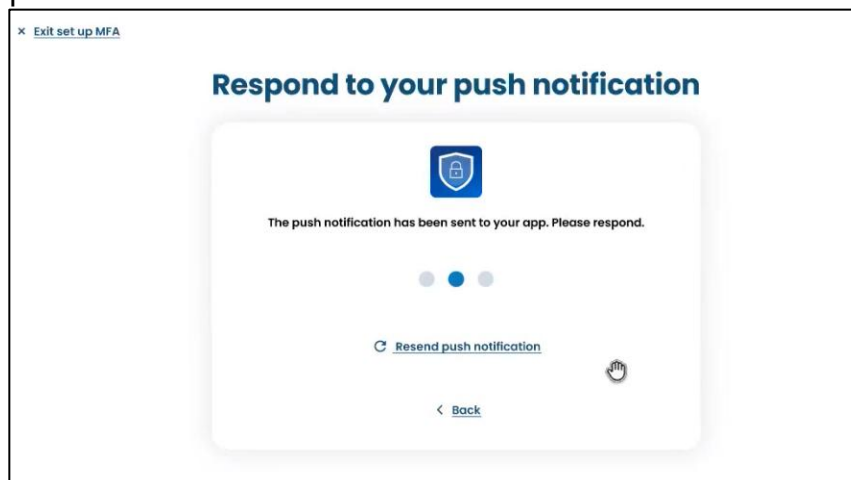


- a. Follow the instructions displayed on the **Set up your ForgeRock Authenticator App** screen to download the ForgeRock application on your device. Scan the **QR code** displayed on the screen. **Do not scan the QR code in this document**
- b. Once the scan is successful, the **Next** button will be enabled. Select 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. Selecting the link will directly open the respective authenticator application.

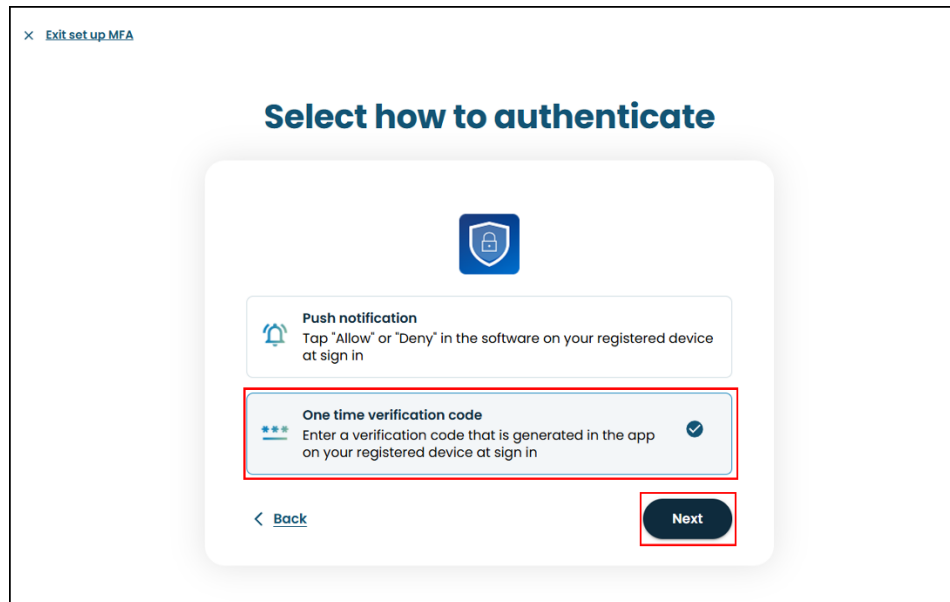
On the **Respond to your push notification** screen, the system displays a loading screen, waiting for you to respond to the notification sent on your mobile app. Select **Allow** on the mobile device to proceed.



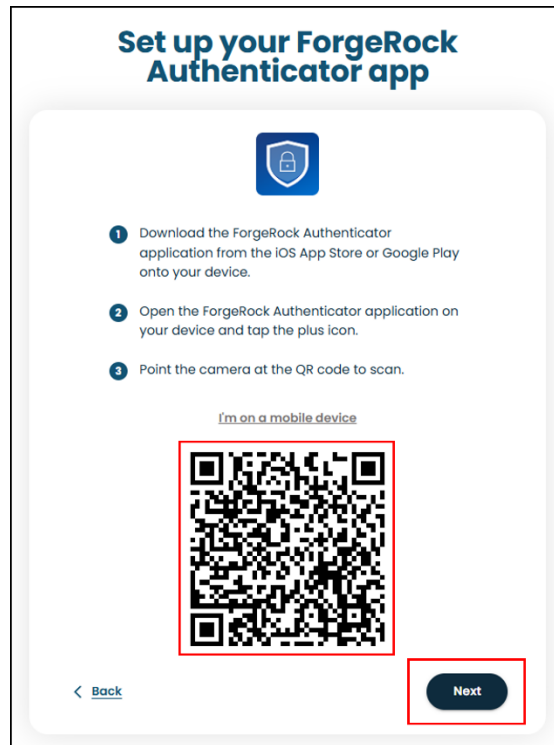
Please note: In case you do not select any response on your mobile phone, then **Resend push notification** link will be enabled. You can select this link to resend the notification or select the **Back** link to go to the previous screen to change the authentication method.

2.2. One time verification code option:

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

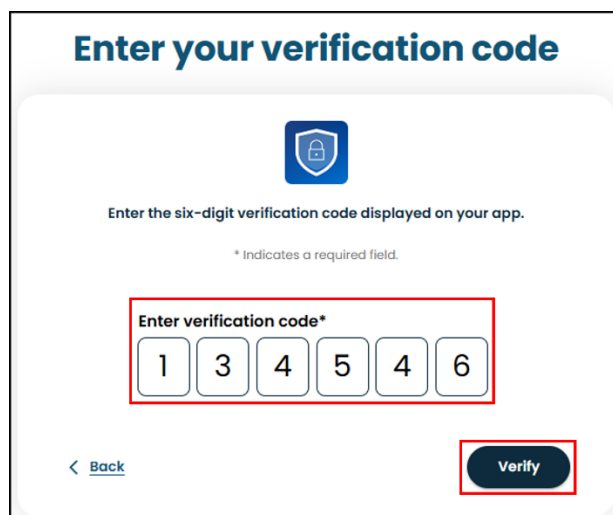


- c. Follow the instructions displayed on the **Set up your ForgeRock Authenticator App** screen to download the ForgeRock application on your device. Scan the **QR code** displayed on the screen.
- d. Once the scan is successful, the **Next** button will be enabled. Select the **Next** button to continue.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



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. Selecting the link will directly open the respective authenticator application.

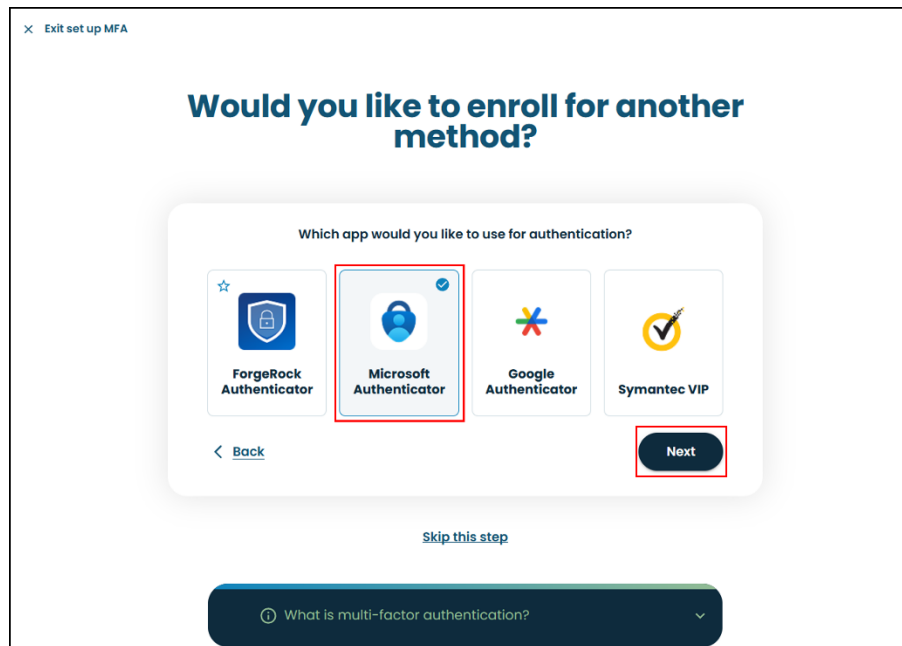
- e. Enter the six digit code sent to the device in the **Enter verification code*** field.
- f. Select **Verify**.



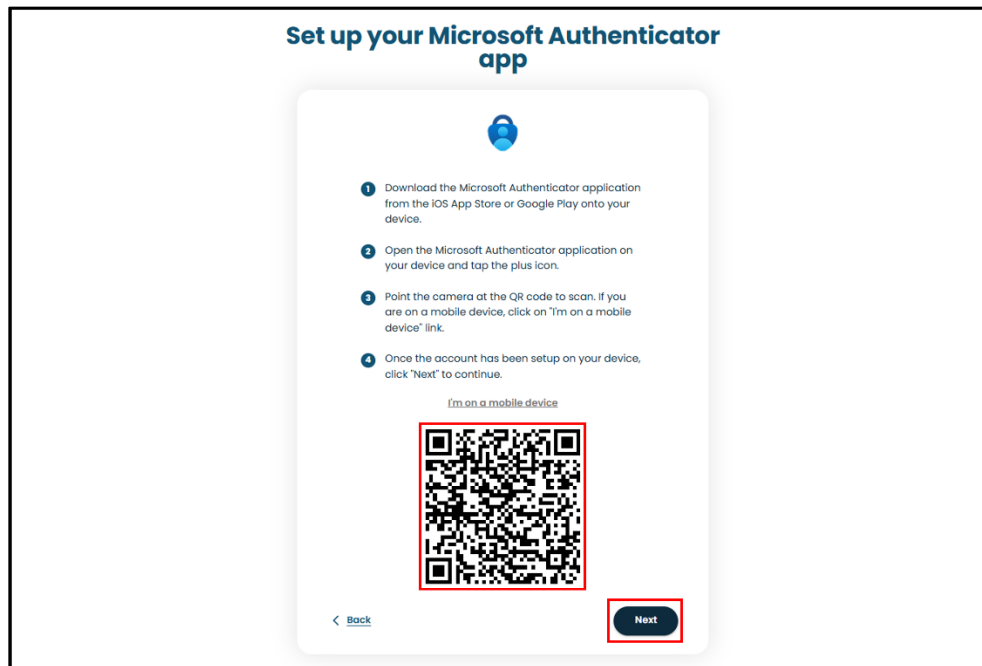
5.1.2 Microsoft Authenticator Application

The Microsoft Authenticator app provides secure account access by generating time-based code 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. Select **Next** to proceed.

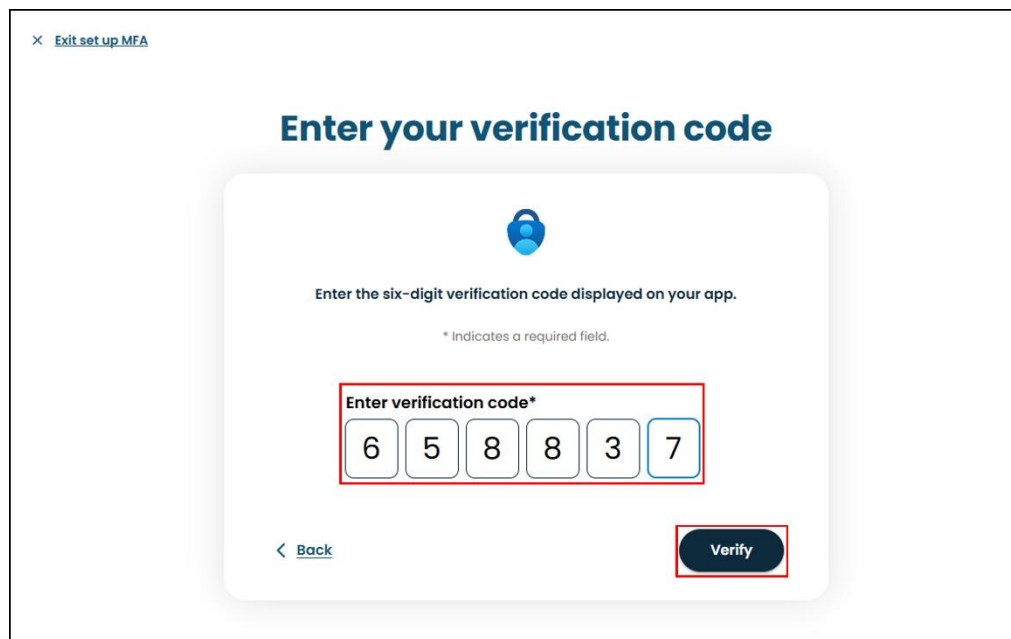


3. Follow the instructions displayed on the **Set up your Microsoft Authenticator App** screen to download the Microsoft application on your device. After the app is installed and ready, scan the **QR code** displayed on the **Set up your Microsoft Authenticator app** screen with the help of your mobile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

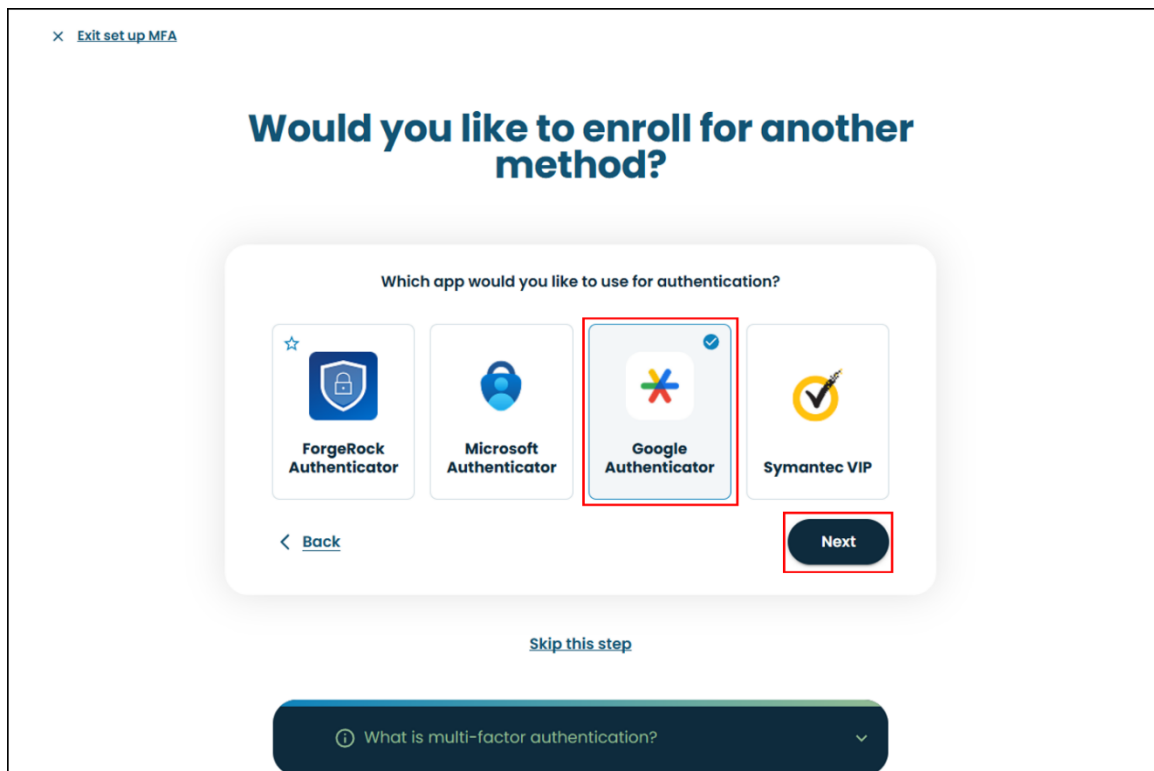
5. In the **Enter the verification code*** field enter the code displayed on the authenticator app on your mobile device.
6. Select **Verify** to proceed.



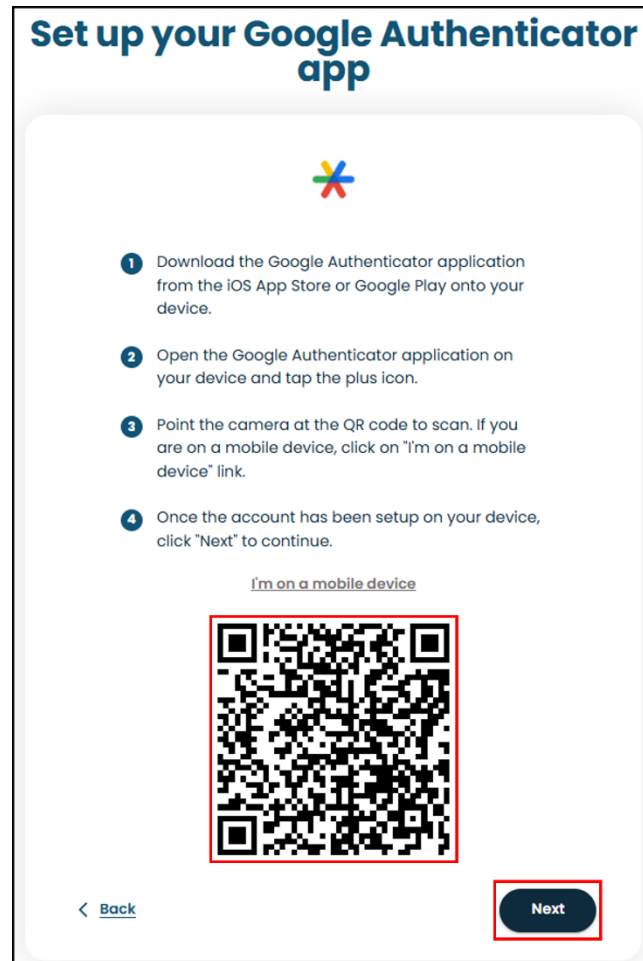
5.1.3 Google Authenticator Application

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. Select **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.
4. Once the scan is successful, the **Next** button will be enabled. Select 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. Selecting the link will directly open the respective authenticator application.

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

Enter your verification code



Enter the six-digit verification code displayed on your app.

* Indicates a required field.

Enter verification code*

1 3 5 4 6 5

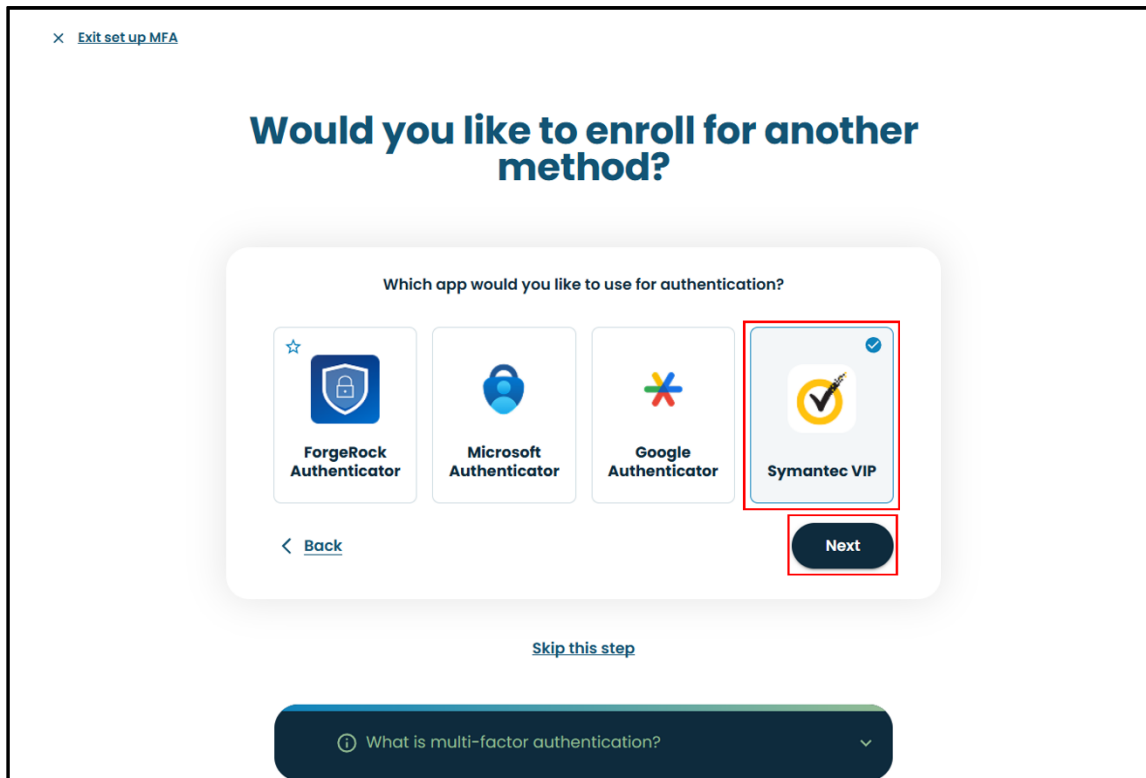
[< Back](#)

Verify

5.1.4 Symantec VIP Application

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. Select **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. Select **Next** to submit the codes.

Setup your Symantec VIP app



- 1 Download and install the Symantec VIP Access app on your mobile device from the App Store or Google Play, or on your desktop from the [Symantec VIP](#) website.
- 2 Open the VIP Access app and follow the on-screen prompts to complete the initial setup.
- 3 When prompted, enter the security code and two consecutive codes generated by your VIP Access app to complete registration.

Enter credential ID

Security code 1

Security code 2

< Back

Next

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

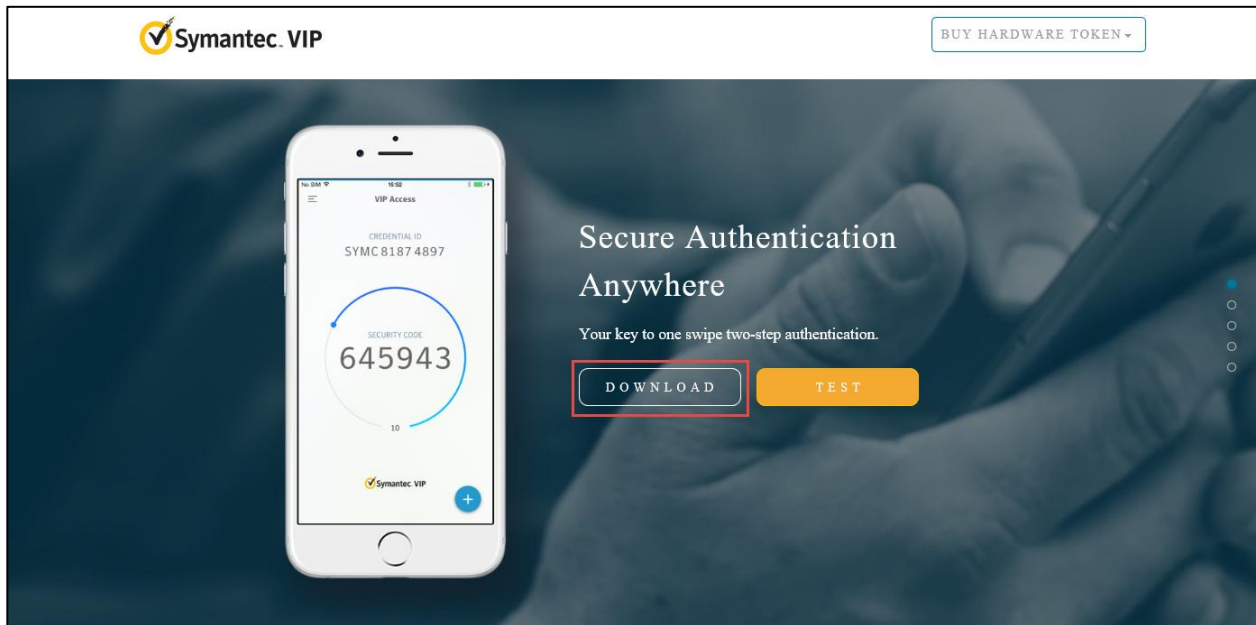
5.1.5 Install Symantec VIP Access Token

If users decide to use Symantec VIP Access Token to access KLOCS and does not have Symantec VIP on their machine or device, users should follow the steps below.

Please note: Users who previously used Symantec VIP to complete MFA will need to re-enroll into Symantec VIP as a one-time activity to continue using this MFA security method. However, users DO NOT need to re-install the app.

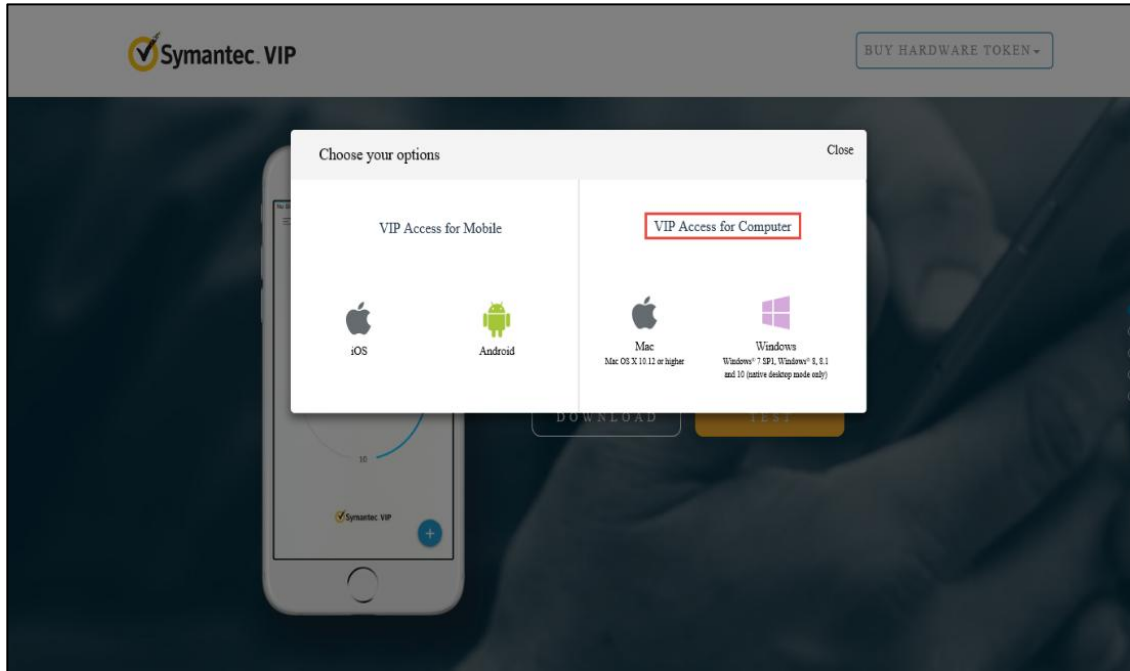
1. Go to <https://idprotect.vip.symantec.com/mainmenu.v> and select **Download**.

Please note: The software is available for desktop and mobile. Please download the required type. To download for a desktop, use the link above and follow the steps below. To download for mobile, download the app from the app store or Google Play on your mobile device.

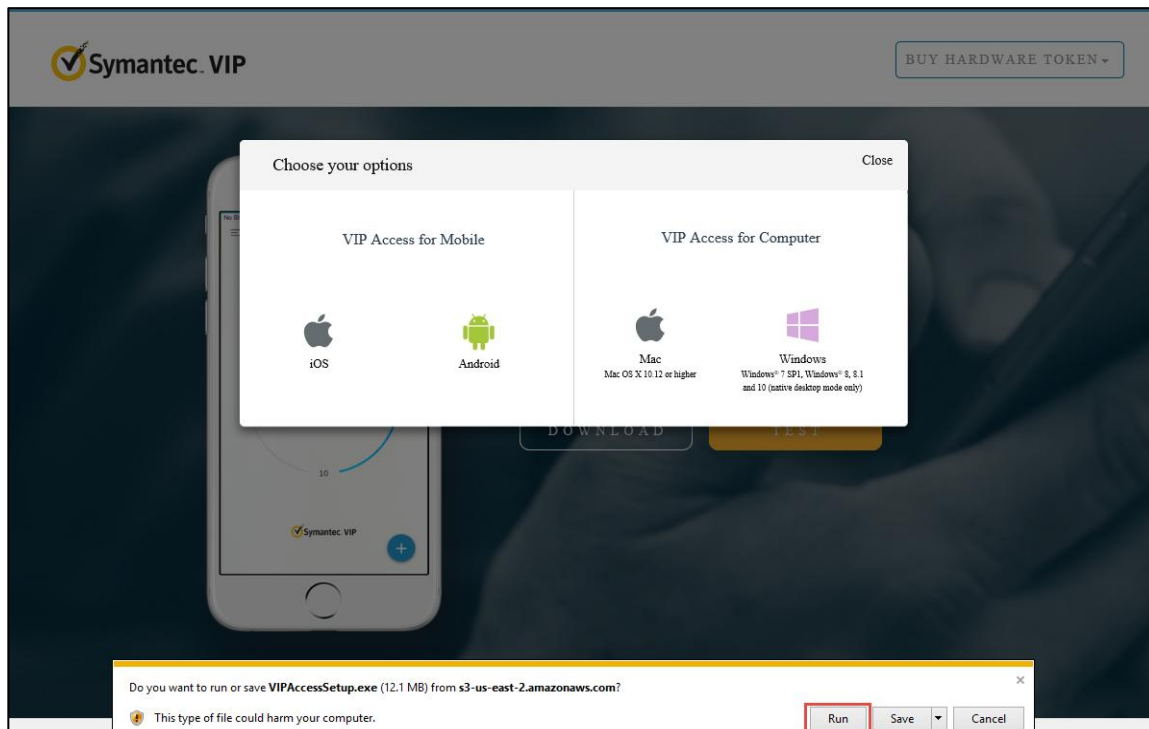


Please note: In some instances, a System Administrator from your Agency may be required to download this software on your behalf.

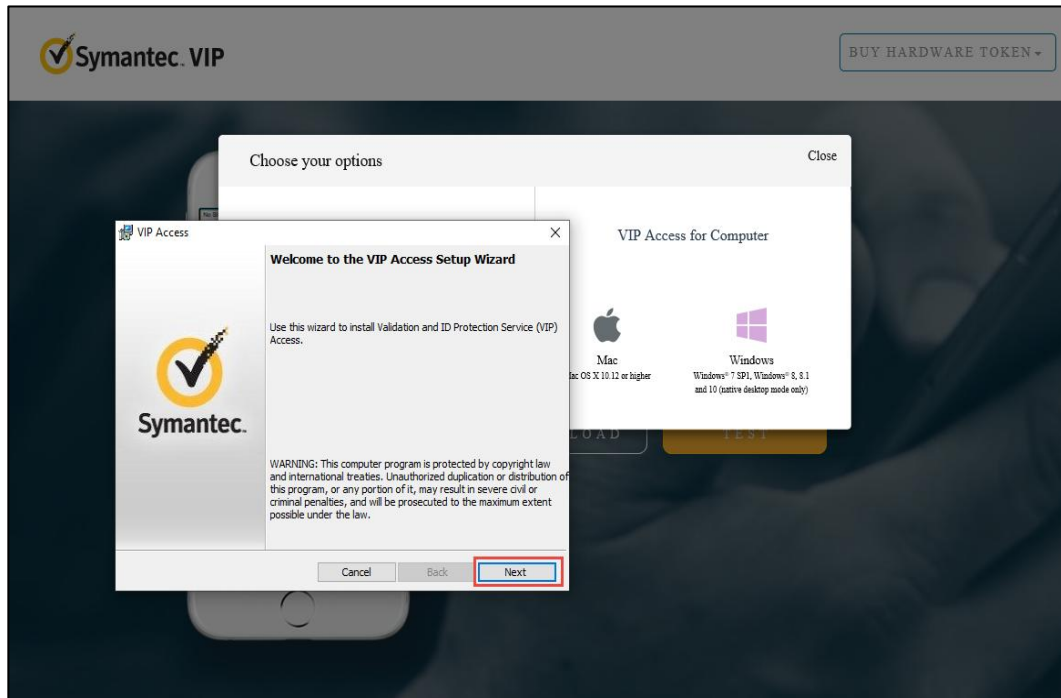
2. To download the Symantec VIP token, choose of the options:
 - To download for Windows-based machine, select **Windows**.
 - To download for Mac, select **Mac**.



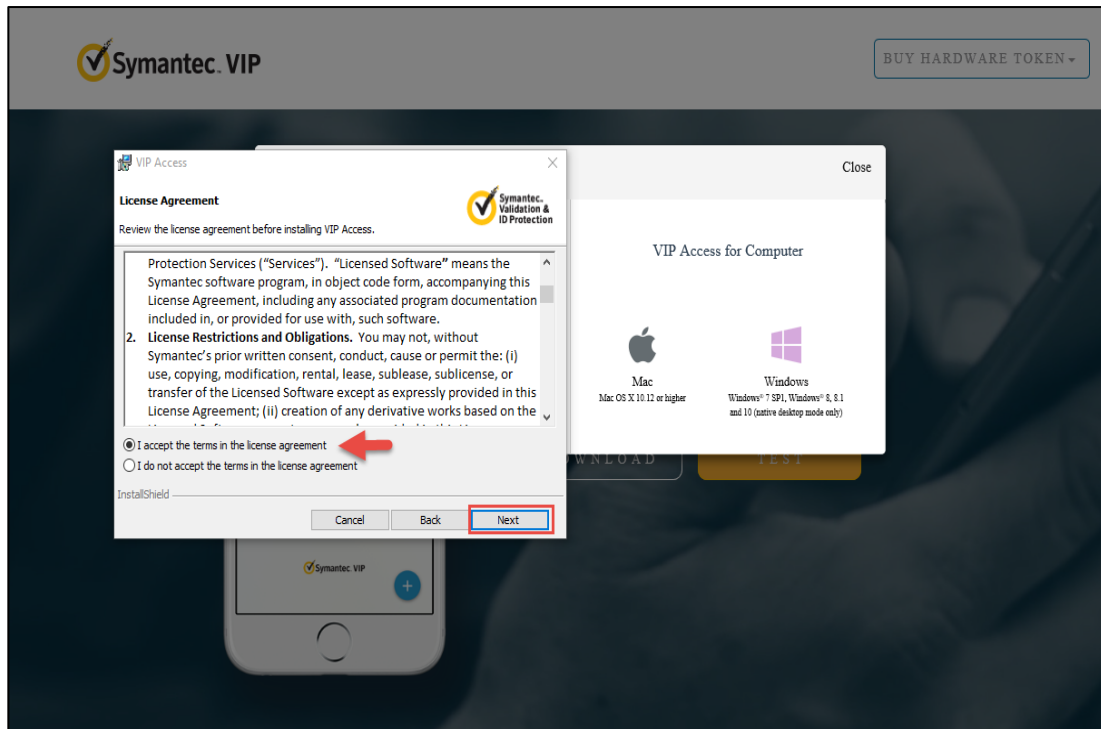
3. Select **Run** to set up VIP Access.



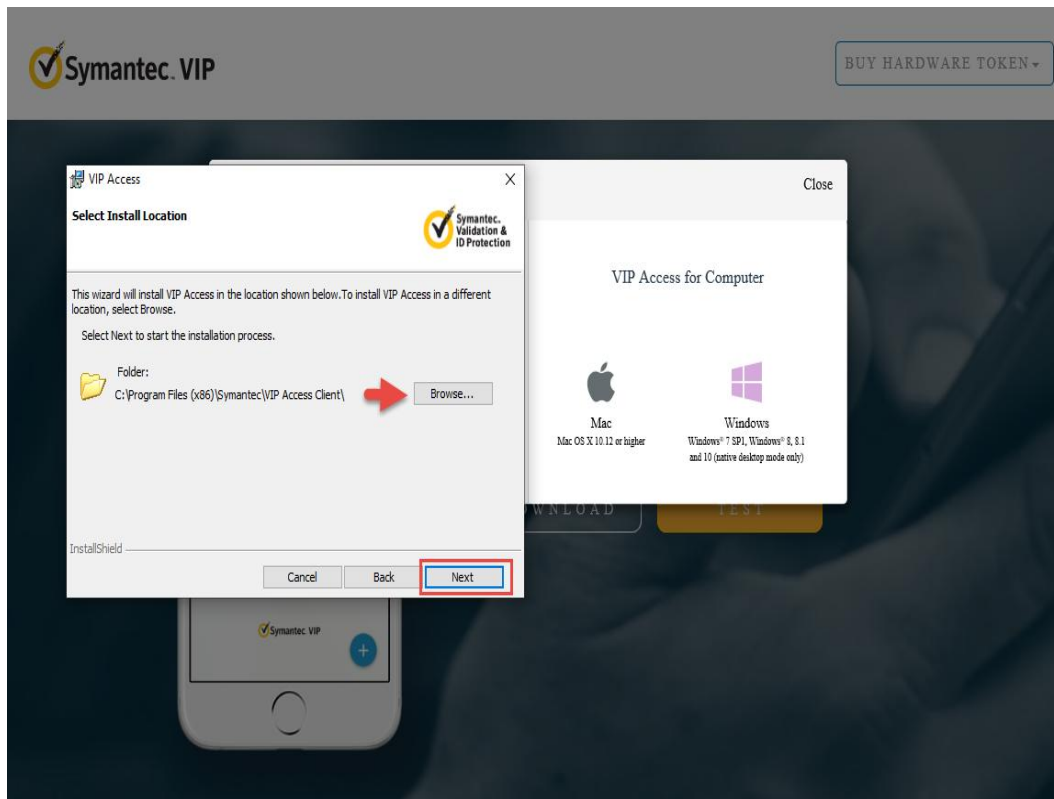
4. Select **Next**.



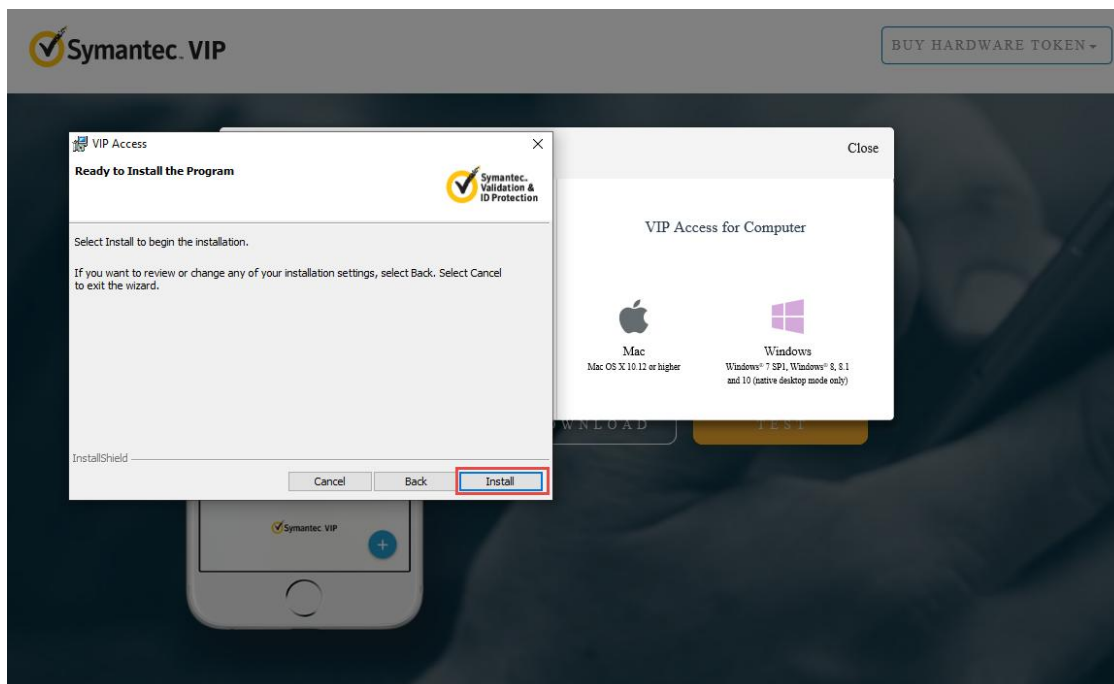
5. Check **I accept the terms in the license agreement** (if the terms are accepted) and select **Next**.



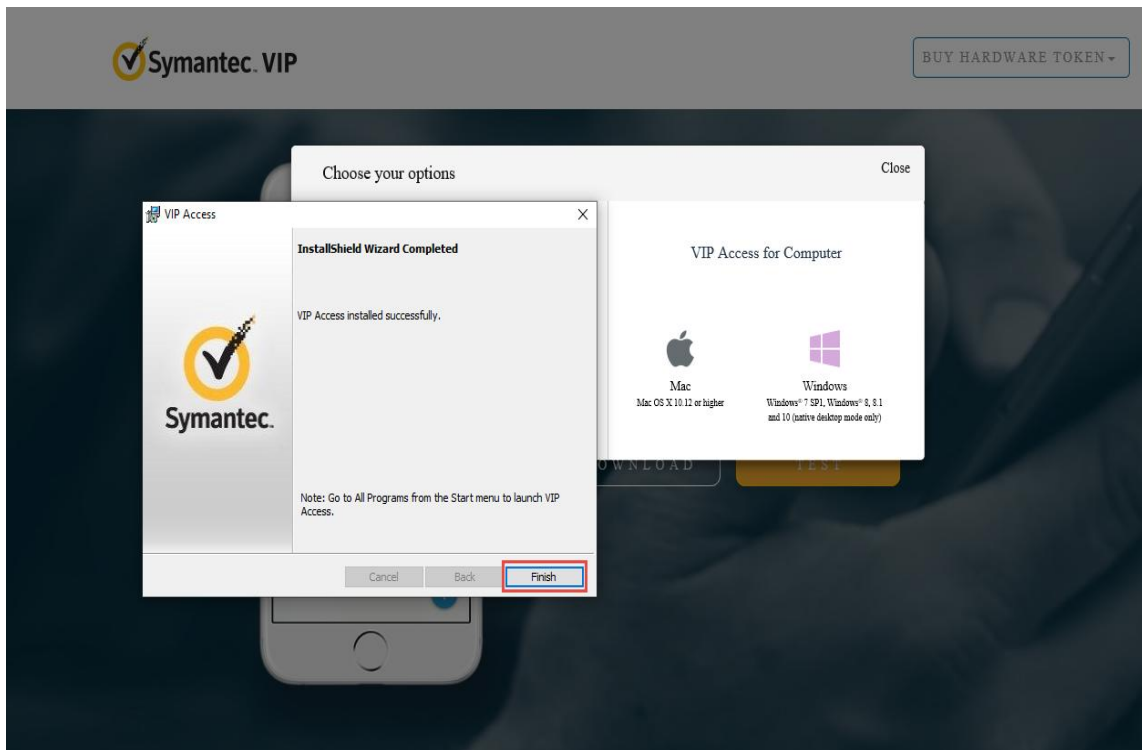
6. Select Install Location and select **Next**.



7. Select **Install** to begin the Installation.



8. Select **Finish**. The VIP Access is installed successfully.



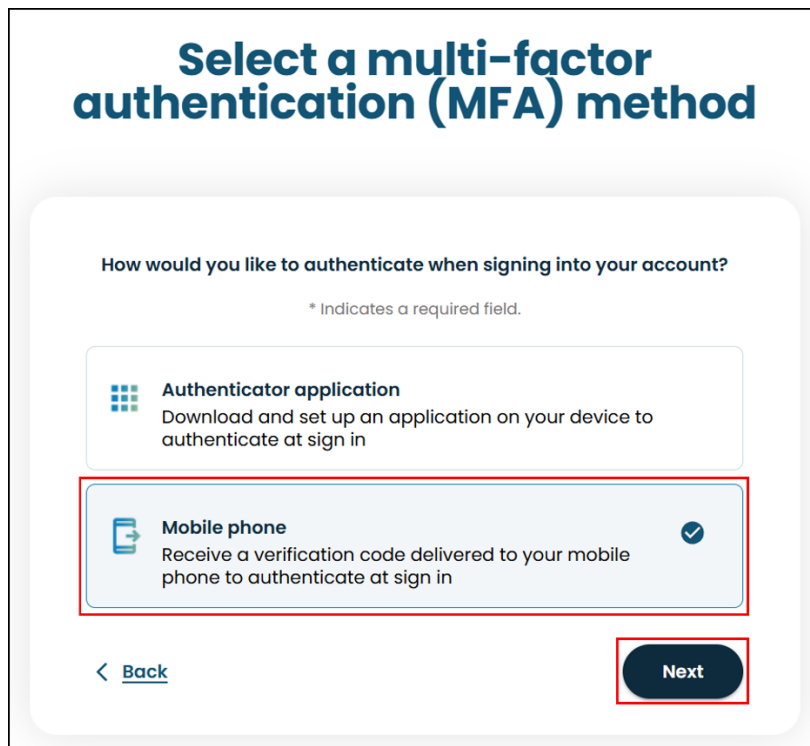
9. The user has successfully registered MFA on their computer. Select on the **VIP Access icon**. In the bottom right on the screen, the VIP Access Credential ID, and Security Code display.



5.2 Set up MFA: Mobile Number Authentication

When logging into KYID for the first time, if the email address and password entered on the KYID login screen are correct, users will be asked to setup their multi-factor authentication. Follow the steps below:

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



Select a multi-factor authentication (MFA) method

How would you like to authenticate when signing into your account?

* Indicates a required field.

Authenticator application
Download and set up an application on your device to authenticate at sign in

Mobile phone
Receive a verification code delivered to your mobile phone to authenticate at sign in

[< Back](#) **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. Select **Next**.

The screenshot shows a mobile number verification form. At the top, there is a 'Country code' dropdown menu set to '(+1) United States'. Below this are two input fields: 'Mobile number' and 'Confirm mobile number', both containing the text '(859) 555-1234'. These two fields are enclosed in a red rectangular box. Below the input fields is a section titled 'How would you like to receive the verification code?'. This section contains two radio button options: 'Text Message' (which is selected, indicated by a blue checkmark) and 'Voice call'. The 'Text Message' option includes a speech bubble icon and the text 'You will receive a passcode via text message to your phone'. The 'Voice call' option includes a telephone handset icon and the text 'You will receive a passcode via voice call to your phone'. This entire selection area is also enclosed in a red rectangular box. Below the selection options, there is a line of text: 'By providing your mobile phone number you are consenting to receive messages (Standard data rates may apply)'. At the bottom of the form, there is a link that says 'Skip this step'. In the bottom left corner, there is a '< Back' link. In the bottom right corner, there is a dark blue button labeled 'Next', which is highlighted with a red rectangular box.

Country code

(+1) United States

Mobile number

(859) 555-1234

Confirm mobile number

(859) 555-1234

How would you like to receive the verification code?

Text Message ✓
You will receive a passcode via text message to your phone

Voice call
You will receive a passcode via voice call to your phone

By providing your mobile phone number you are consenting to receive messages (Standard data rates may apply).

[Skip this step](#)

< [Back](#) **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, select **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.

Verify your mobile number

Six-digit verification code was sent to +1 (859) 555-1234. Enter the verification code provided to verify your mobile number.

* Indicates a required field.

Enter verification code*

3 2 7 4 8 5

Code expires in 04:31 minutes

Verify

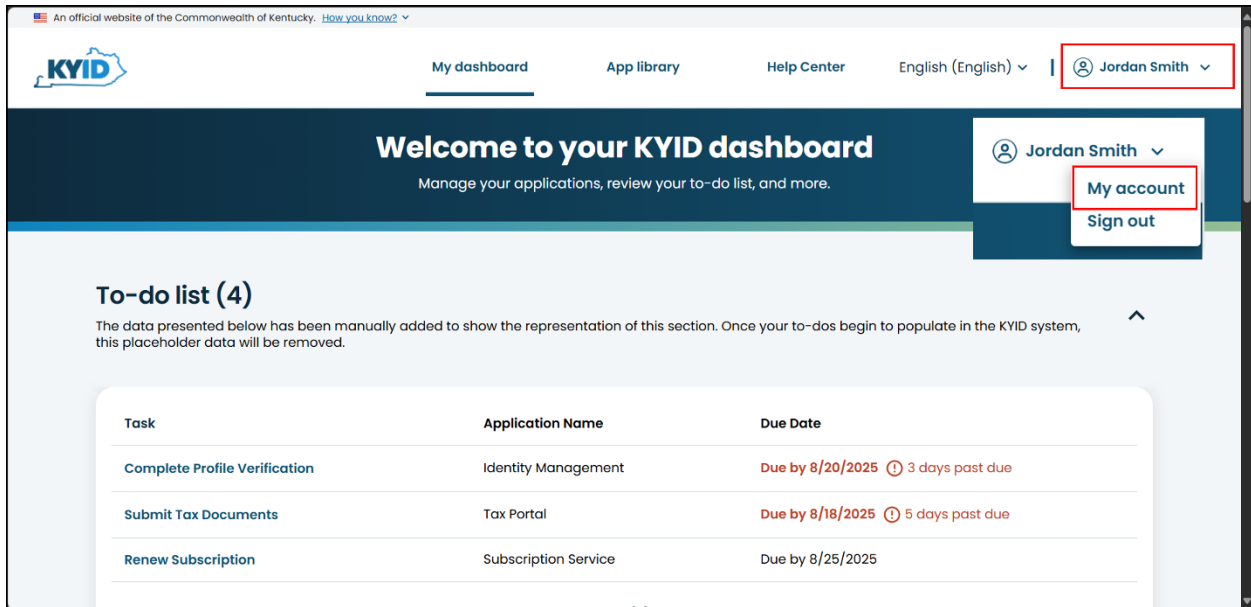
Resend verification code by [text message](#) or [voice call](#)

[< Back](#)

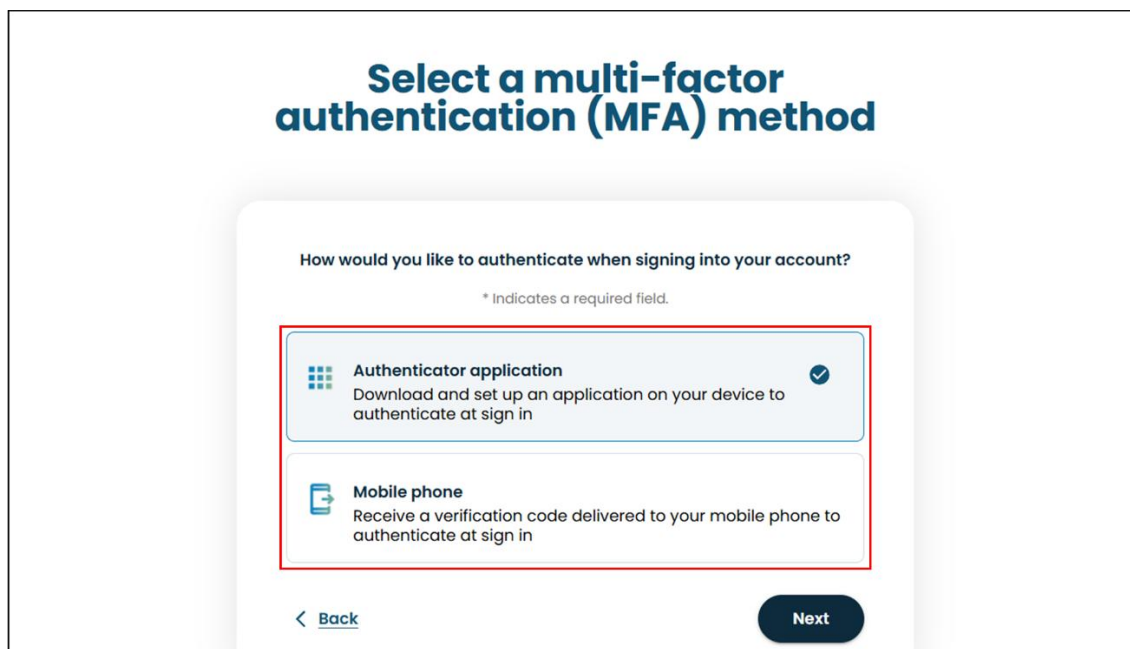
5.3 Add/Remove MFA Security Methods

Resetting Multi-Factor Authentication (MFA) allows you to regain access to your account if you lose your authentication device or need to reconfigure your security settings. By following the steps below, you can securely reset your MFA and set up a new authentication method.

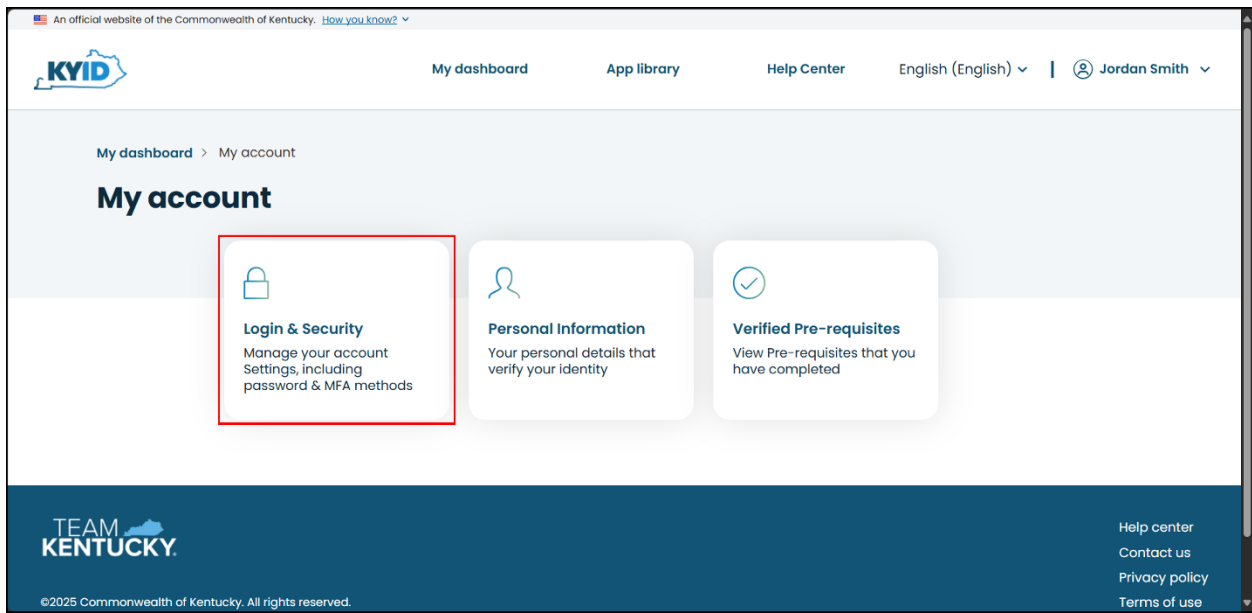
1. Login into the KYID platform with the help of your existing credential details. On the dashboard, select the **Username** drop down in the top right corner of the screen.
2. Select **My account** from the menu.



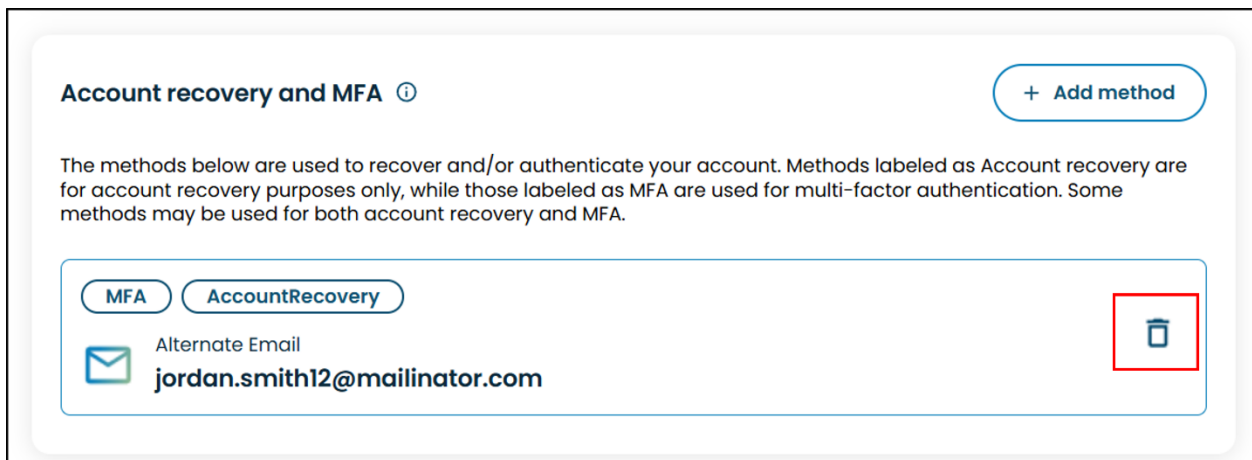
3. Complete the MFA option you have set up on your account.



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



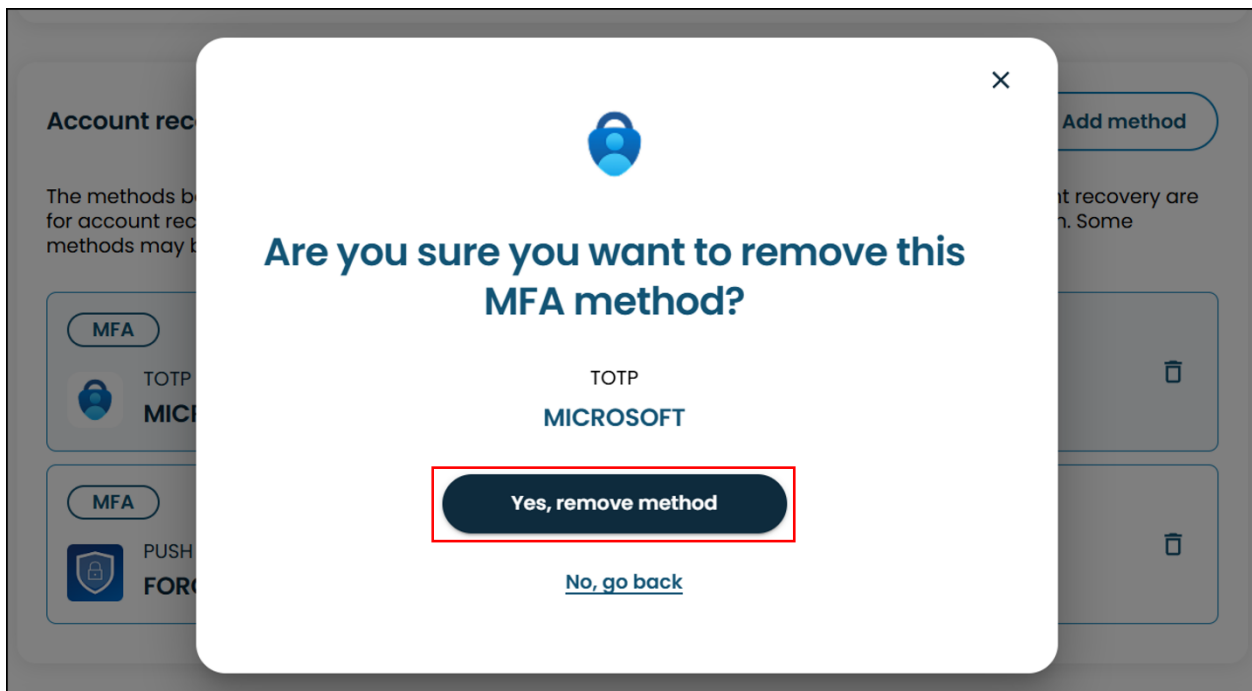
5. Scroll down to review the **Account recovery and MFA** tile on this screen.
6. Select the **trash** icon next to an MFA method you want to remove.



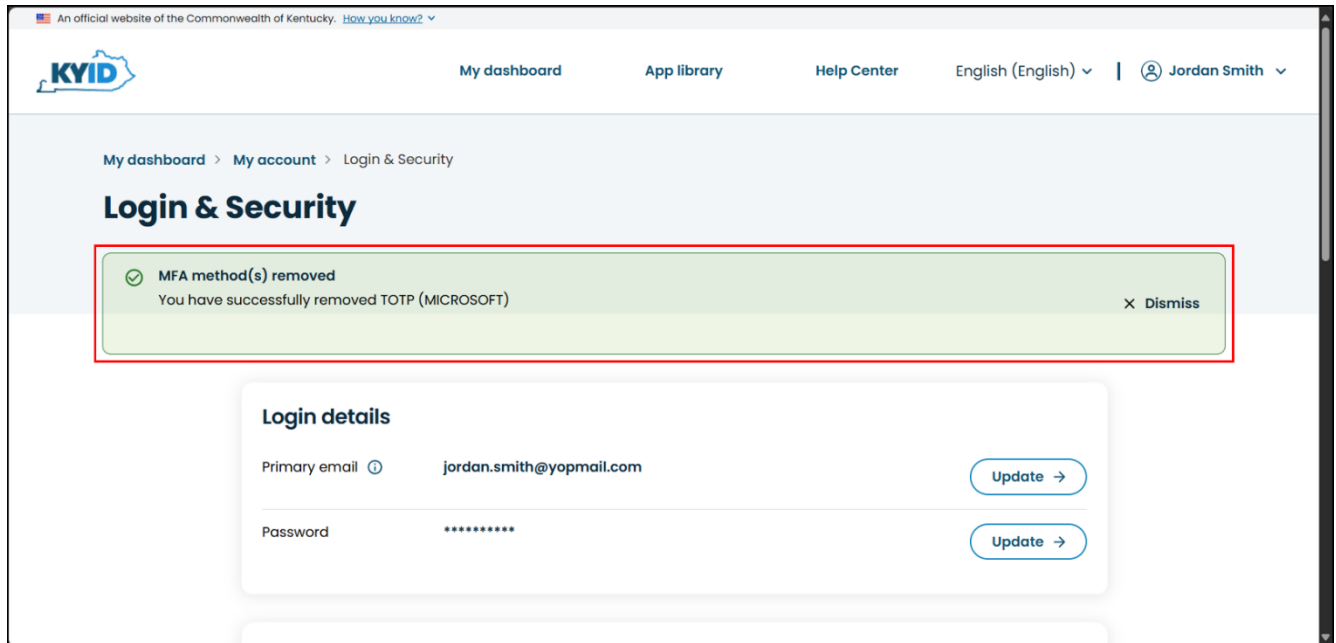
Please note: The **Account Recovery and MFA** section displays the methods available for recovering and authenticating your account. Methods labeled **Account Recovery** are used solely for account recovery, while those labeled **MFA** are used for multi-factor authentication. Some methods may serve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

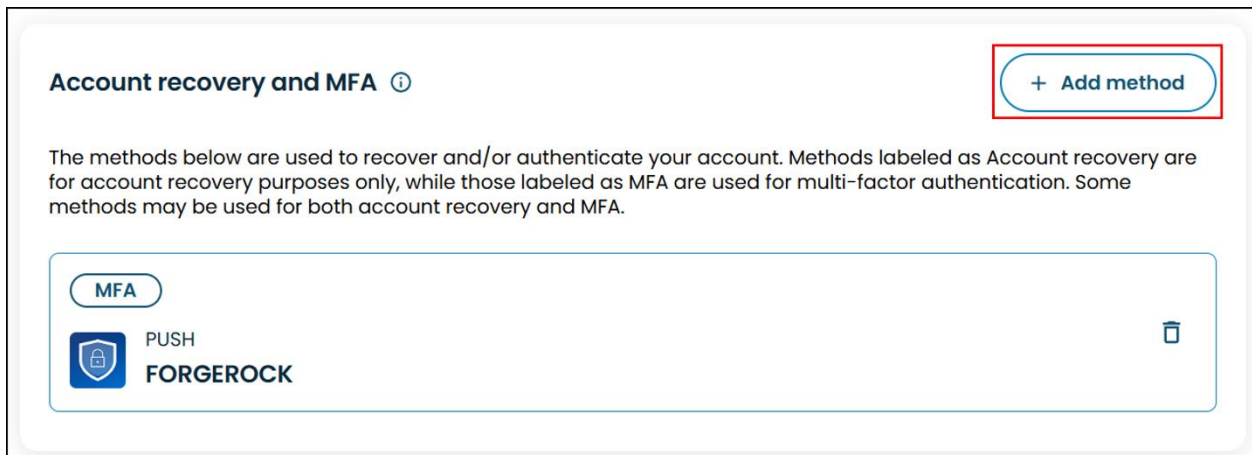
7. Select **Yes, remove method** on the **Are you sure you want to remove this MFA method** popup.



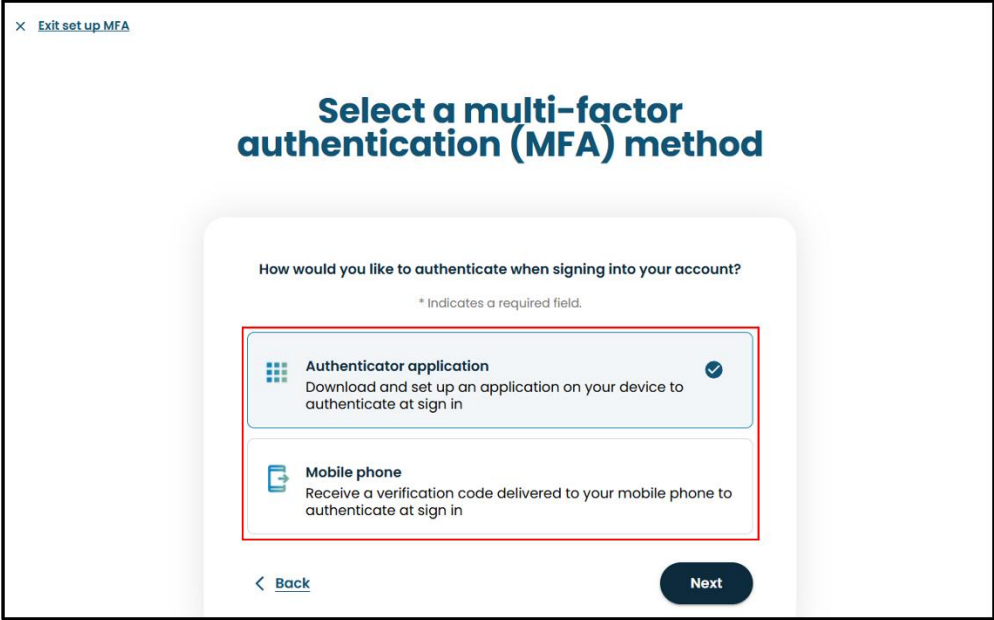
- When the selected MFA method is removed successfully, a message will be displayed on the screen with the message: **You have successfully removed an MFA method.**



- To set up a new MFA method, select the **+ Add method** button and then follow the steps in the [Setting Up Your Authenticator Application](#) section of this QRG.



10. The **Select a multi-factor authentication (MFA) method** screen appears. Follow the same steps in the section [5.1 Set up MFA: Via Authentication Application](#) and/or [5.2 Set up MFA: Via Mobile Phone](#).



The screenshot shows a mobile application interface for selecting an MFA method. At the top left, there is a close button (X) and a link "Exit set up MFA". The main heading is "Select a multi-factor authentication (MFA) method". Below this, a question asks "How would you like to authenticate when signing into your account?". A small note states "* Indicates a required field." Two options are presented in a list: "Authenticator application" with a grid icon and a checkmark, and "Mobile phone" with a phone icon. Both options are enclosed in a red rectangular border. The "Authenticator application" option includes the instruction "Download and set up an application on your device to authenticate at sign in". The "Mobile phone" option includes the instruction "Receive a verification code delivered to your mobile phone to authenticate at sign in". At the bottom, there are "Back" and "Next" navigation buttons.

× [Exit set up MFA](#)

Select a multi-factor authentication (MFA) method

How would you like to authenticate when signing into your account?

* Indicates a required field.

**Authenticator application**
Download and set up an application on your device to authenticate at sign in

**Mobile phone**
Receive a verification code delivered to your mobile phone to authenticate at sign in

< [Back](#) [Next](#)

6 Login Instructions

Agents should proceed with the following steps to log into the system:

1. Navigate to <https://kyid.ky.gov>.
2. Enter the **Email Address** and select **Next**.

The screenshot shows the KYID website's sign-in interface. On the left, a large heading reads "All your applications, one secure place." Below it, a subheading states "Through KYID, you can access all your Kentucky applications—simply and securely." A "Create Account" button is visible. On the right, a "Sign In" box contains the following elements: a note "* Indicates a required field.", an "Email*" input field with the text "jordan.smith@mailinator.com", a checkbox labeled "I consent to the System Notice" which is checked, a "Next" button, and a "Forgot email" link. The top of the page includes the KYID logo, a "Help Center" link, a language dropdown set to "English (English)", and a "Sign in" link.

3. Enter the **Password** and select **Sign In**.

This screenshot shows the same KYID sign-in page, but at the password entry stage. The "Email*" field now contains "existing.user@yopmail.com". The "Password*" field is masked with dots. The "Next" button has been replaced by a "Sign In" button, and a "< Back" link has been added below it. The "Forgot Password" link remains at the bottom. The rest of the page layout, including the heading and navigation links, is identical to the previous screenshot.

Please note: If any application within KYID requires Multi-Factor Authentication (MFA), users are prompted to complete MFA when logging into KYID, rather than when accessing the specific application.

The system redirects the user to complete Multi-Factor Authentication through ForgeRock, Microsoft, Google, Symantec VIP, or phone, depending on the MFA the user has enrolled in. Complete the required steps for MFA.