Enrolling in
Multi Factor Authentication (MFA)
to Access the TRAQS Website and API

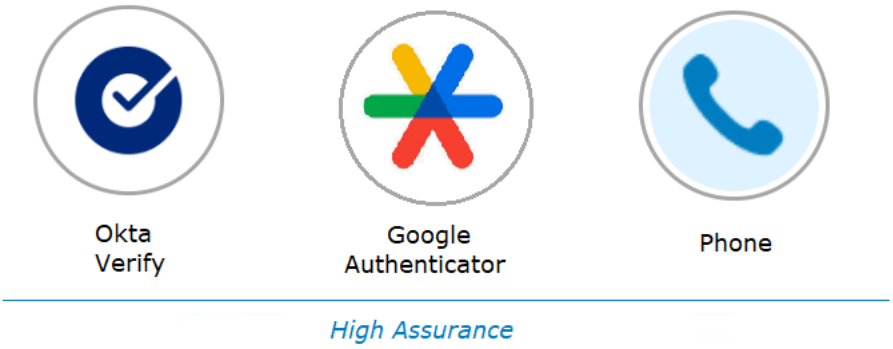
APRIL 29, 2024 – VERSION 2.0

The information contained herein may not be copied, retransmitted, disseminated, distributed, sold, resold, leased, rented, licensed, sublicensed, altered, modified, adapted, or stored for subsequent use for any such purpose, in whole or in part, in any form or manner or by any means whatsoever, to or for any person or entity, including the purchaser, without FINRA's express prior written consent (unless such use constitutes fair use under the Copyright Act).

Multi Factor Authentication (MFA) enhances the security of accounts by adding an additional layer of security beyond the Username and password. All users of the TRAQS website are required to enroll in MFA using their mobile device or landline. Sharing account credentials is not recommended.

The following enrollment steps only need to be completed once per user account. For more information about MFA please see our TRAQS MFA website.

The TRAQS website uses a combination of Transport Layer Security (TLS) encryption and an Okta cloud based authentication platform referred to as the NASDAQ MFA Service to protect data that is being transferred from the client to FINRA and back. To access the TRAQS website for trade reporting, the user must be entitled to use the product, have an assigned Username and password, answer the security questions and have at least one second factor authentication method. The available second factor authentication methods include Okta Verify, Google Authenticator, and Phone (SMS Authentication and Voice Call Authentication).

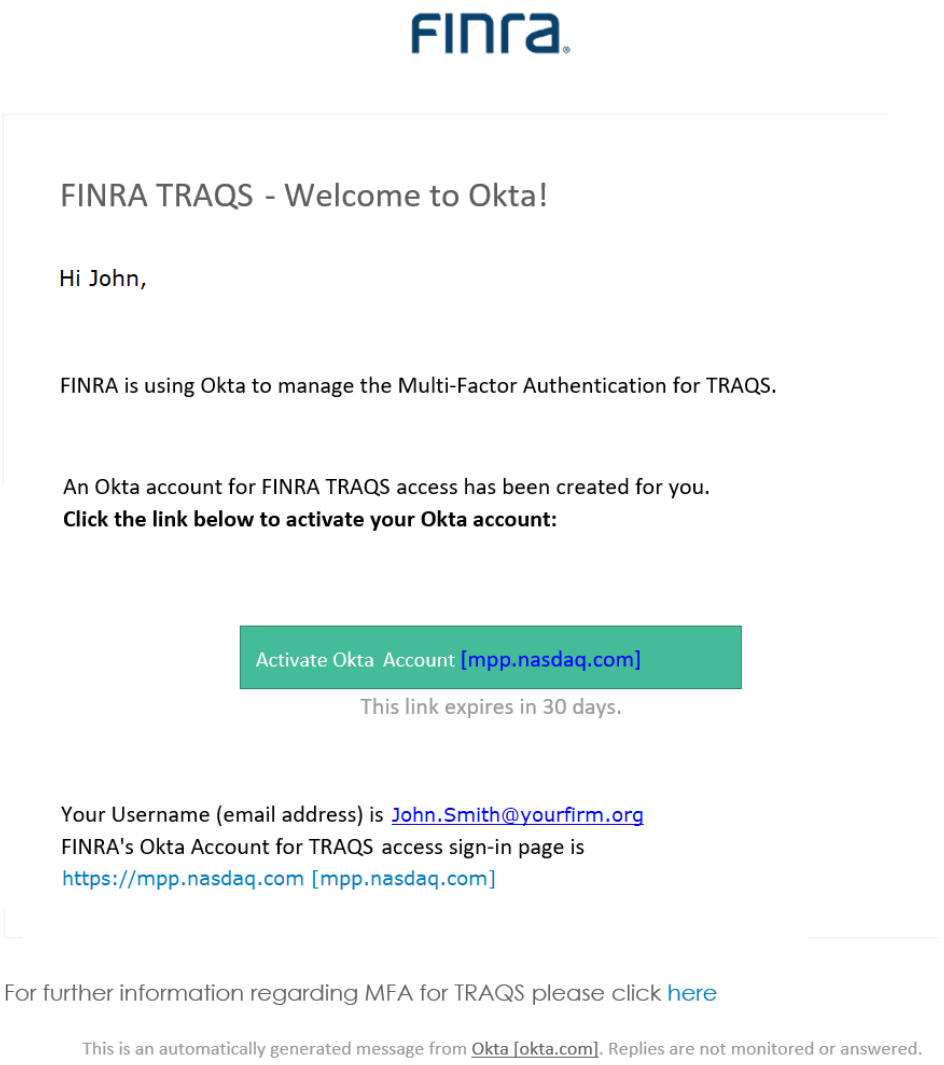


Note: This guide covers information specific to MFA. Review the TRAQS User Guide for the trade reporting product for questions about navigating the TRAQS website.

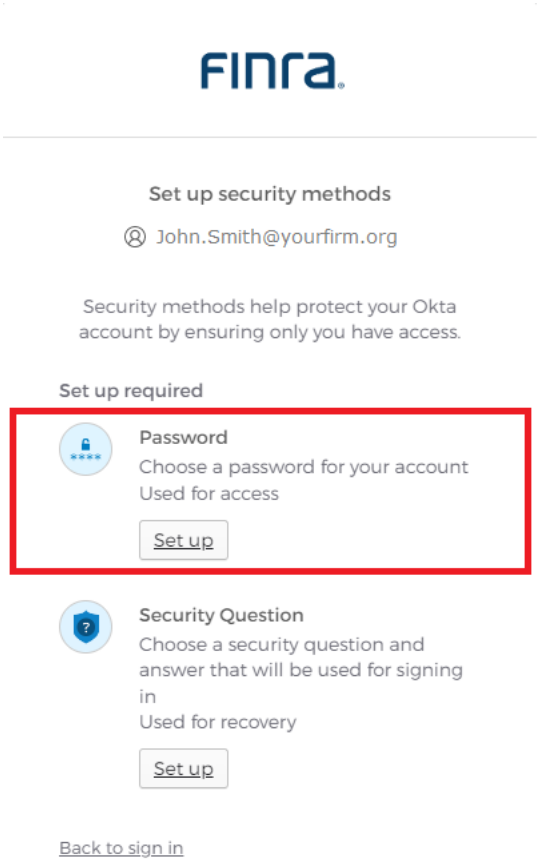
Table of Contents

Section 1: How to Enroll and Choose Authentication Method(s) to Access the TRAQS Website

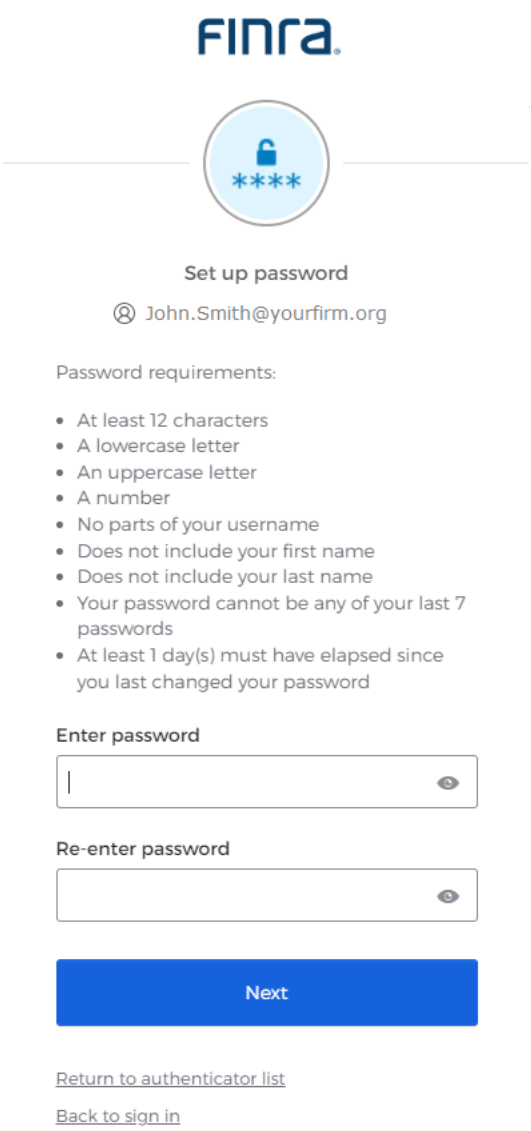
1. To establish a new TRAQS Username, please use the **Participant Data Management System**.
2. An email will be sent to the user containing an invitation to access the NASDAQ MFA service.
3. Click on the **Activate Okta Account** link in the email. This will allow you to set up your Okta Account for TRAQS. The Okta Account set up involves **setting up a password, security question/answer and preferred authentication methods**.



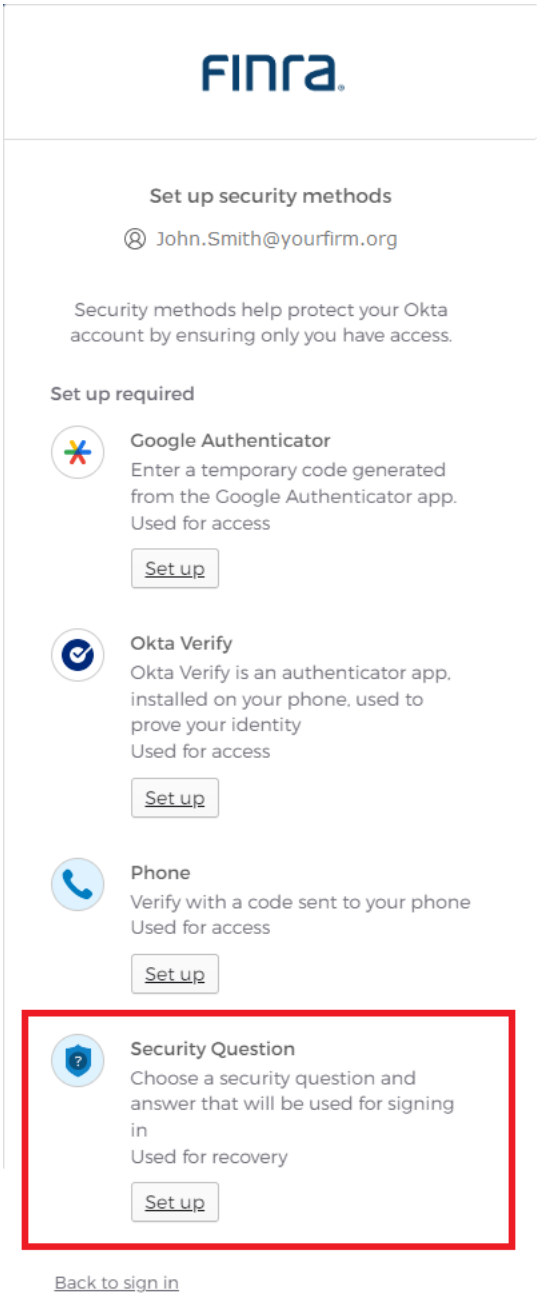
4. Under **Password,** click **Set up**.



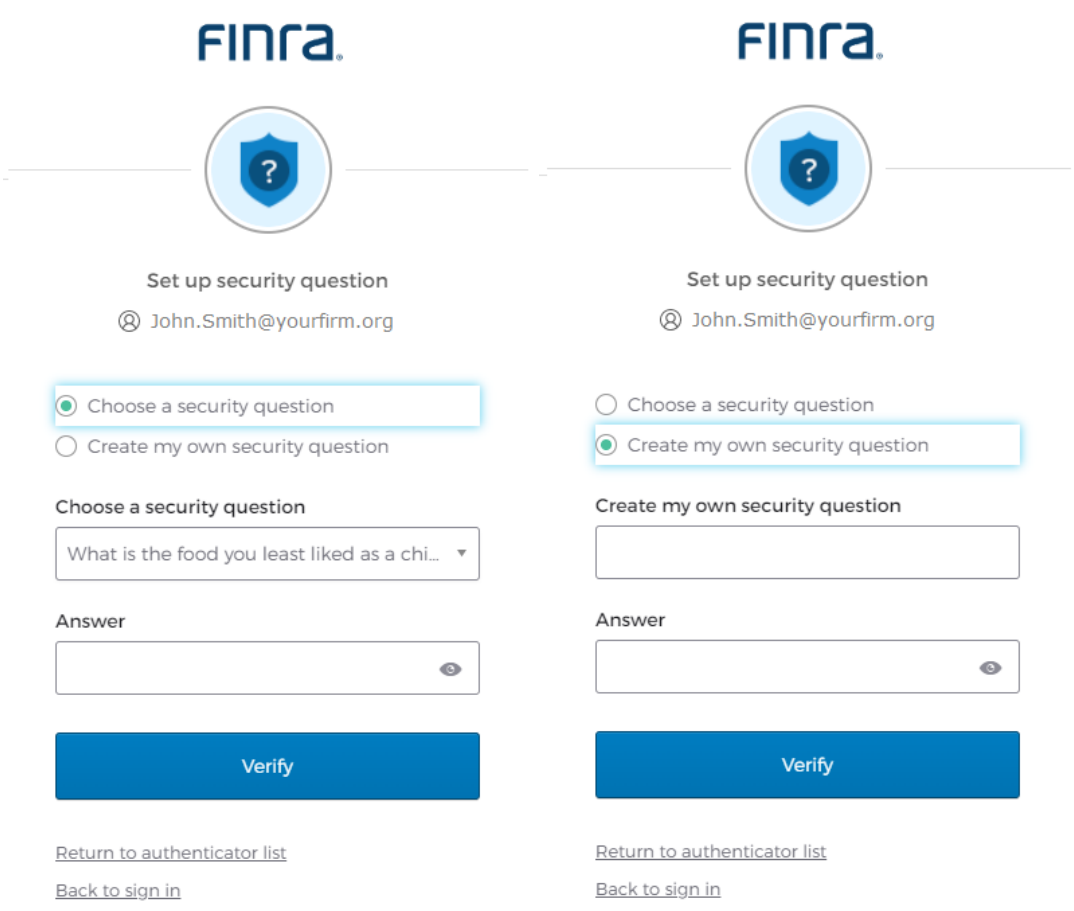
5. **Enter a Password,** confirm your password in the **Re-enter Password** field, click **Next.**



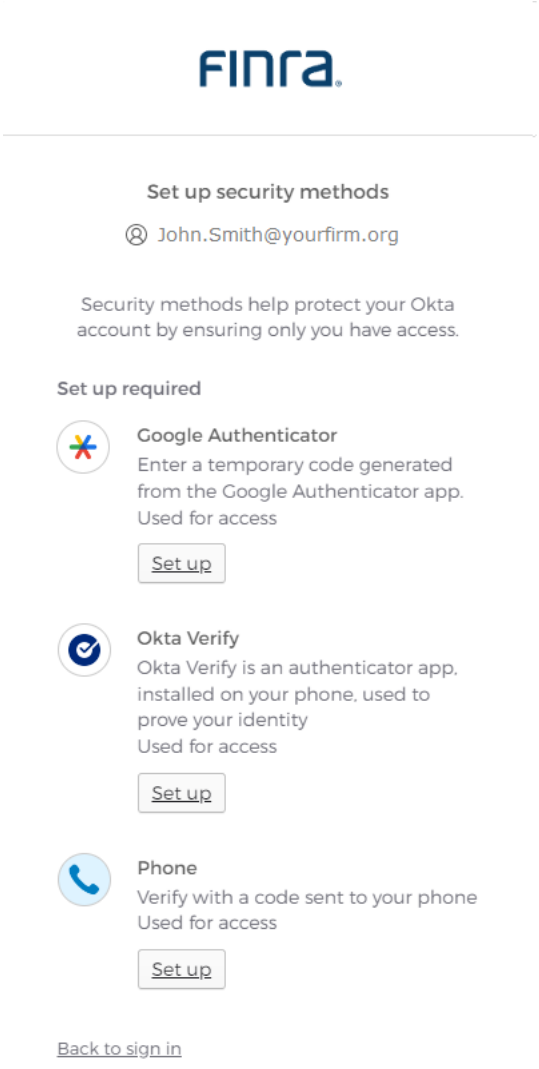
6. Under **Security Question,** click **Set up**.



7. Select which security question you want to set up, **Choose a security question** and enter your **Answer** -OR- select **Create my own security question**, type in your own security question in the text box and enter your **Answer**. The answer must be at least 3 characters. Click **Verify.**



8. Select the **Preferred Authentication Method** from the list of available choices including: **Google Authenticator, Okta Verify, or Phone (SMS Authentication or Voice Call Authentication)**. Please continue reading for a description of each authentication method and instructions for enrollment. **Note:** FINRA recommends that users enroll in more than one authentication method to allow for redundancy if your mobile device is unavailable. FINRA suggests enrolling in voice call authentication using a phone number that differs from your mobile device as a backup.

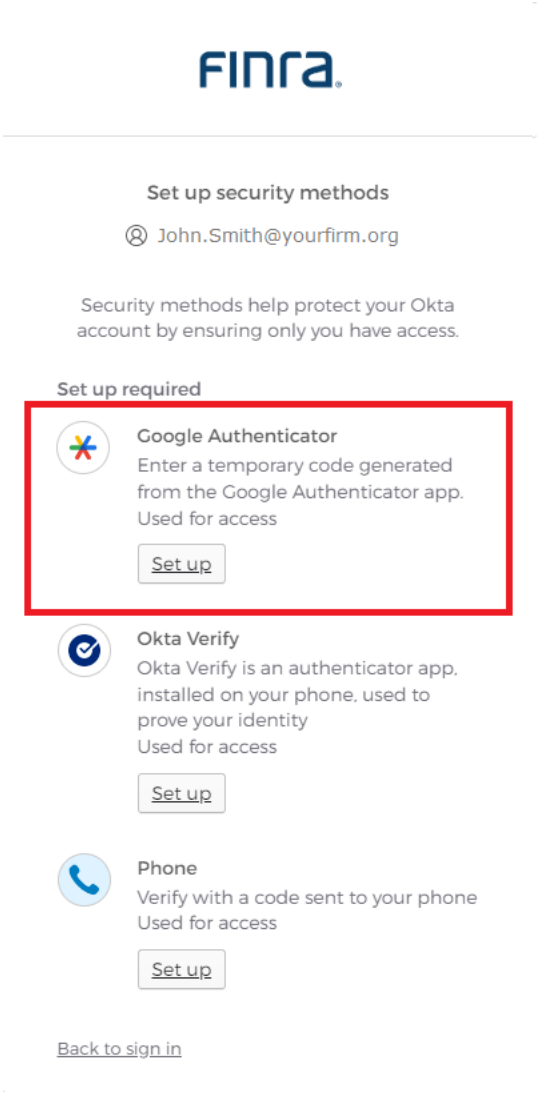


Google Authenticator

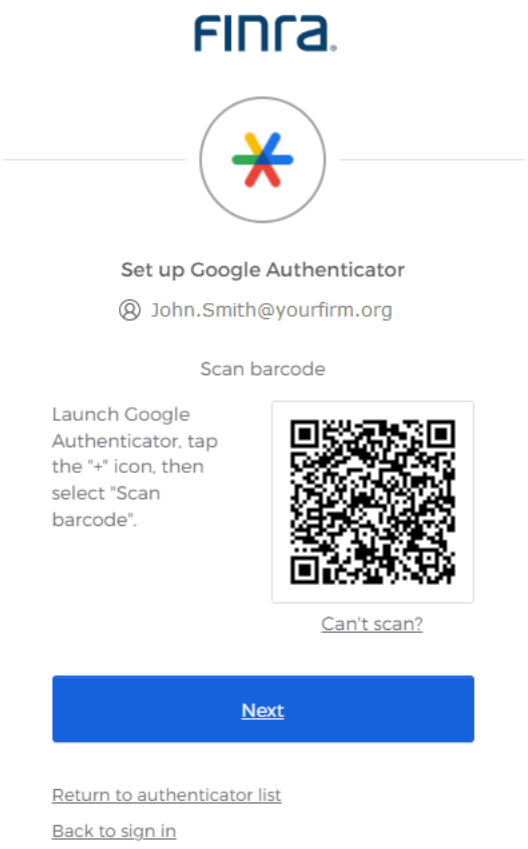
This method of verification uses a third-party app to generate a 6-digit code for users to type into the Sign In screen. Users will have 30 seconds to input the code before it generates another.

Setting up Google Authenticator

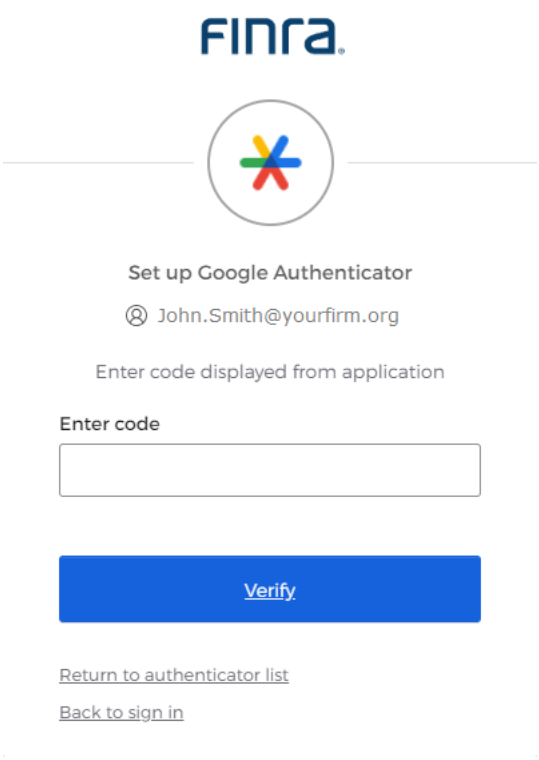
1. **Download** the **Google Authenticator App** from the App Store (iPhone), Google Play or Blackberry World Store (Android devices) onto your primary mobile device.
2. Under **Google Authenticator,** click **Set up**.



3. A **QR Code** will appear on your computer monitor.
4. **Open** the **Google Authenticator App** on your mobile device and follow the instructions to add FINRA's MFA.
5. **Scan** the **Barcode** using the **Google Authenticator App,** click **Next**.



6. **Enter the code** from your mobile device without spaces onto the screen, click **Verify**. Please note that the code changes every 30 seconds. If you fail to enter a code within 30 seconds, please enter the next generated code.



7. Once you have completed the verification set up, you will be directed back to the **Preferred Authentication Method** screen with rest of available verification choices. Please continue reading for a description of each authentication method and instructions for enrollment.
8. Select **Set up later** if you are finished setting up your authentication methods. Please see How to Remove My Security Methods for information about removing Security Methods.
9. Users can choose to add additional factors or proceed directly to the TRAQS website. Please see Section 3 for instructions on logging into the TRAQS website using MFA.
10. The website will prompt you to use your chosen security method(s) to login.

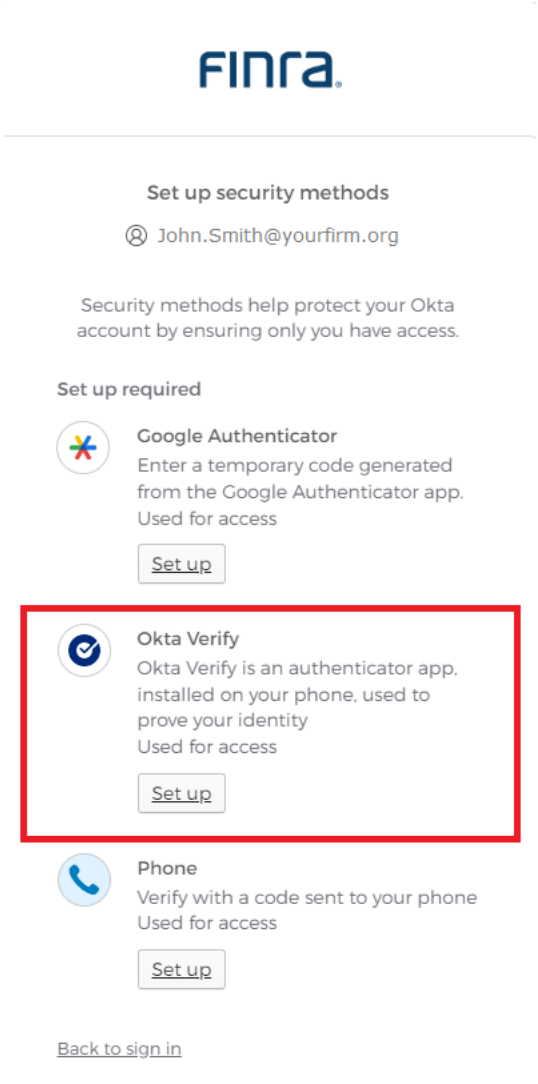
Okta Verify

This is a mobile app that verifies your identity in one of two ways. Okta Verify can send a push notification that you approve on your mobile device. Alternatively, Okta Verify can generate a 6-digit code that displays for users to type into the Sign In screen.

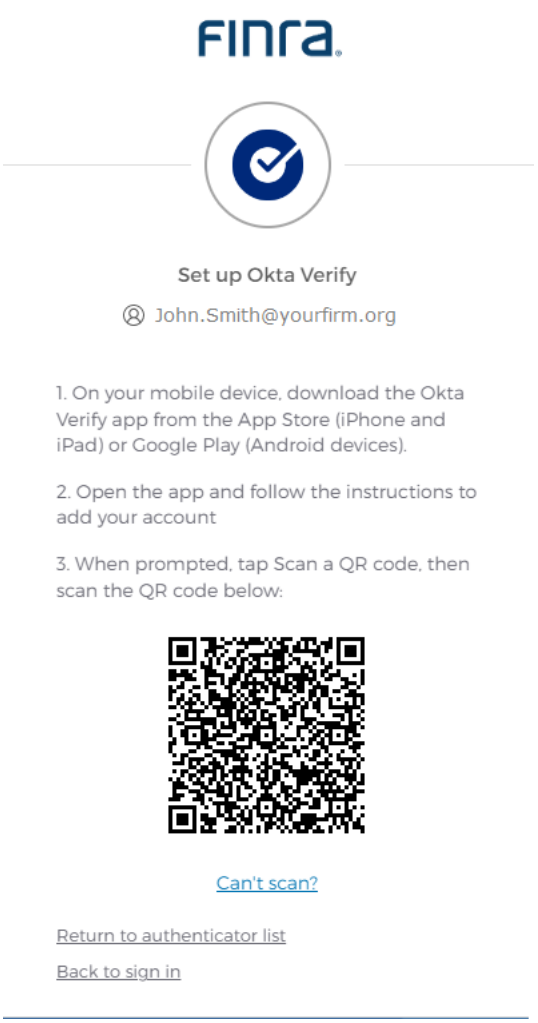
Note for iPhone users: If you would like to use Okta verify, you must have face id/touch id (iPhone 5 and higher) enabled on your phone. If you do not want to enable face id/touch id please use another verification. Also you must be on the latest iOS.

Setting up Okta Verify

1. **Download** the **Okta Verify App** from the App Store (iPhone), Google Play or Blackberry World Store (Android devices) onto your primary mobile device.
2. Under **Okta Verify,** click **Set up**.



3. A **QR Code** will appear on your computer monitor.
4. **Open** the **Okta Verify App** on your mobile device and follow instructions to add FINRA's MFA.
5. **Scan** the **Barcode** using the **Okta Verify App.**

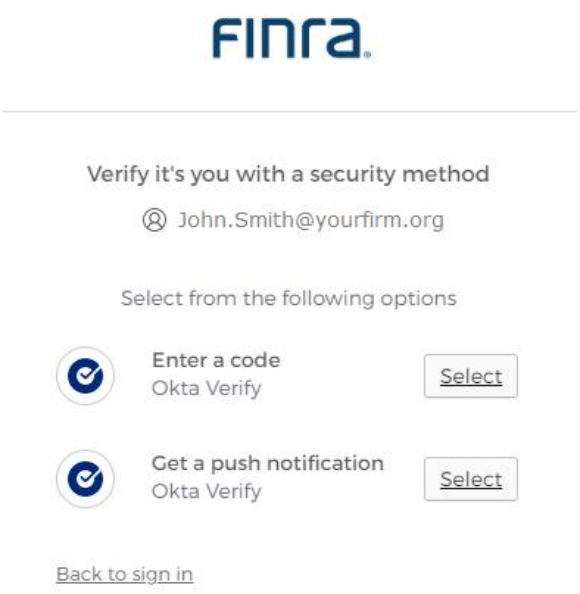


6. Once you have completed the verification set up, you will be directed back to the **Preferred Authentication Method** screen with rest of available verification choices. Please continue reading for a description of each authentication method and instructions for enrollment.
7. Select **Set up later** if you are finished setting up your authentication methods. Please see How to Remove My Security Methods below for information about removing Security Methods
8. Users can choose to add additional factors or proceed directly to the TRAQS website. Please see Section 3 below for instructions on logging into the TRAQS website using MFA.

9. The website will prompt you to use your chosen security method(s) to login.

Note: The user can choose between two Okta Verify verifications, a **code notification** OR **push notification**.

Code: Use an auto generated Okta verify code. Users must enter the code contained in the App into the entry box and click Verify. **Note:** The code changes every 30 seconds. If you fail to enter a code within 30 seconds, please enter the next generated code.	**Push**: Access the Okta Verify app on the associated device and approve the request.

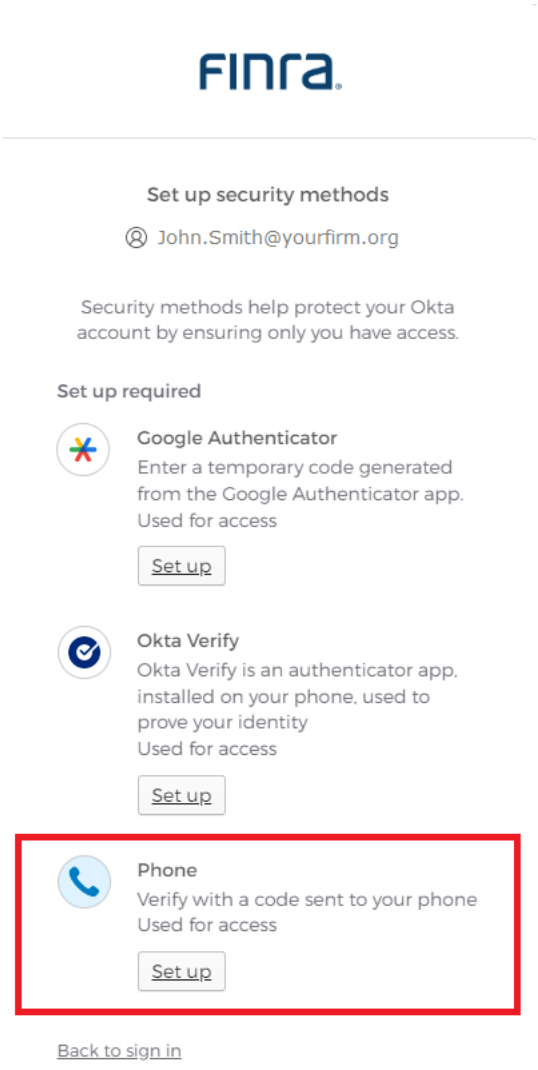


SMS Authentication (Phone)

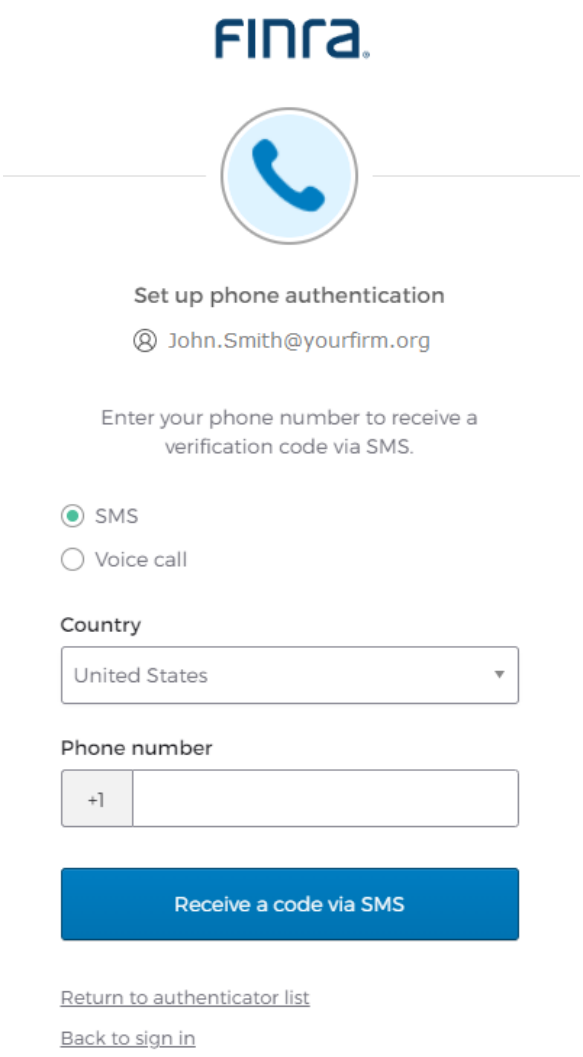
SMS Authentication uses the text messaging service on your mobile device to generate a 6-digit-code for users to type into the Sign In screen.

Setting up SMS Authentication

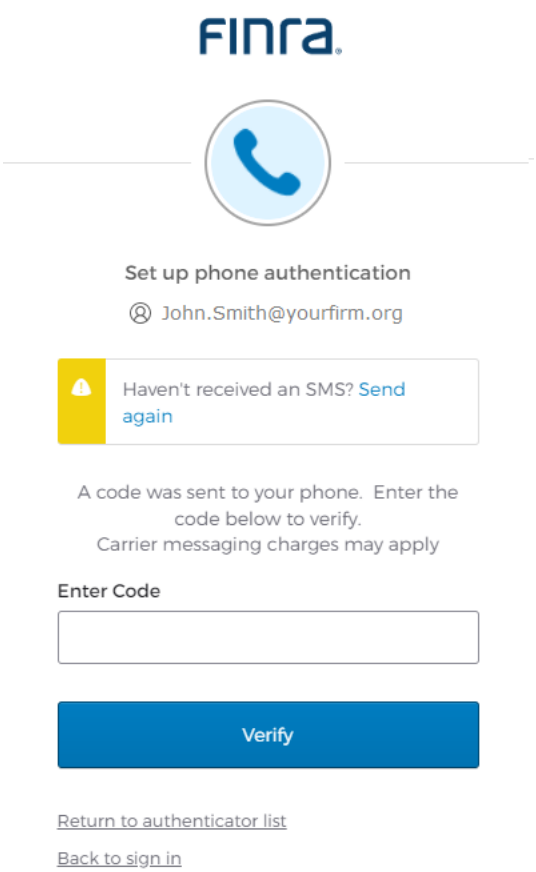
1. Under **Phone,** click **Set up**.



2. Select **SMS, Select your Country** from the drop-down list and **enter your mobile phone number**. The default country is the United States. Click, **Receive a code via SMS**.



3. **Enter the code** that arrives via text message on your mobile device, click **Verify.** If you do not receive the code via SMS, click the **Send again** link.



4. Once you have completed the verification set up, you will be directed back to the **Preferred Authentication Method** screen with rest of available verification choices. Please continue reading for a description of each authentication method and instructions for enrollment.
5. Select **Set up later** if you are finished setting up your authentication methods. Please see How to Remove My Security Methods below for information about removing Security Methods.
6. Users can choose to add additional factors or proceed directly to the TRAQS website. Please see Section 3 below for instructions on logging into the TRAQS website using MFA.
7. The website will prompt you to use your chosen security method(s) to login.

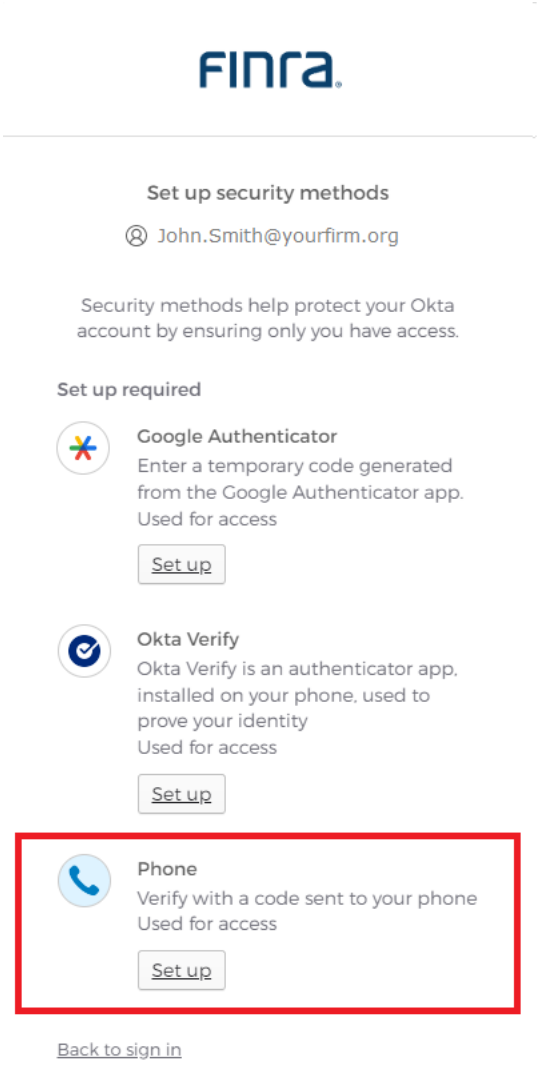
Note: The user must have access to the mobile device associated with the phone number in order to login using this authentication method

Voice Call Authentication (Phone)

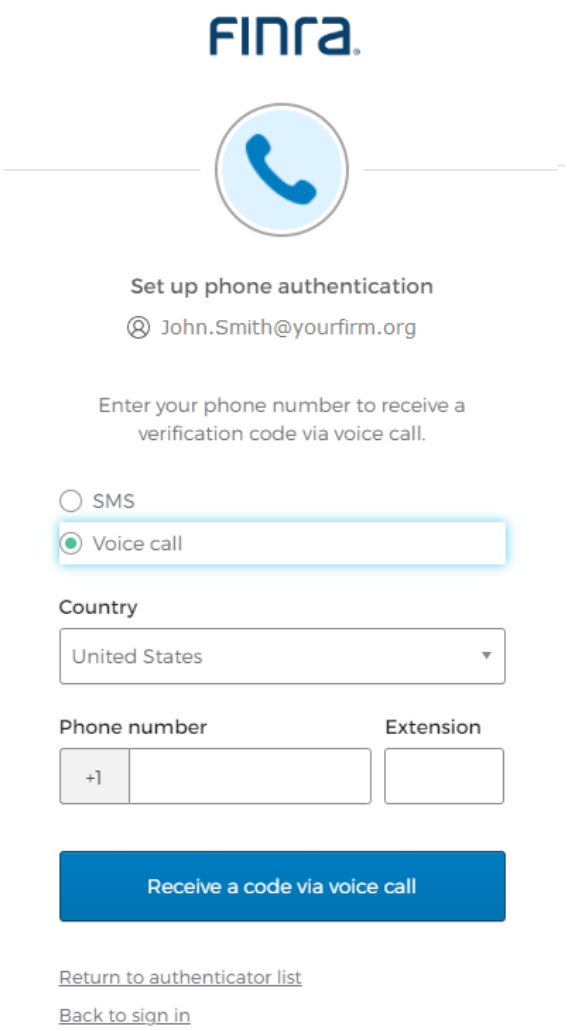
This method of verification will provide a spoken 5-digit-code for users to type into the Sign In screen via mobile device or land line. This method of verification is suitable for users that do not have access to text messaging. This is also the preferred back up authentication type. Please enroll in this method using a phone that differs from your original authentication method.

Setting up Voice Call Authentication

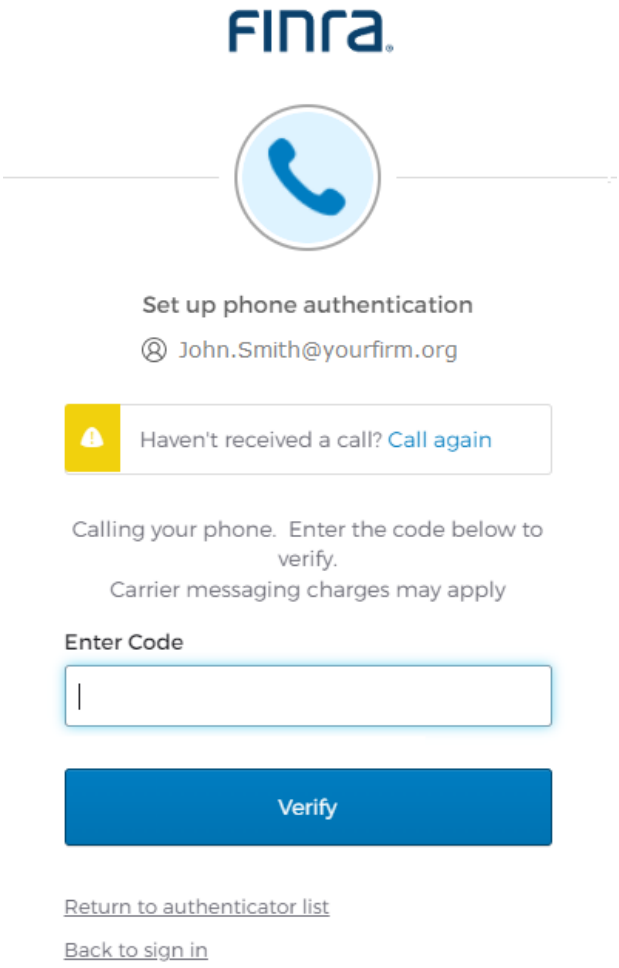
1. Under **Phone,** click **Set up**.



2. Select **Voice Call, Select your Country** from the drop-down list and **enter your phone number**. The default country is the United States. Click, **Receive code via voice call**.



3. **Answer the phone** and follow phone call instructions to authenticate.
4. **Enter the provided code** into the Enter code box. Click **Verify**. **Note:** The call will last about 30 seconds and the code will be repeated twice. If you do not receive the code via a voice call, click the **Call again** link.

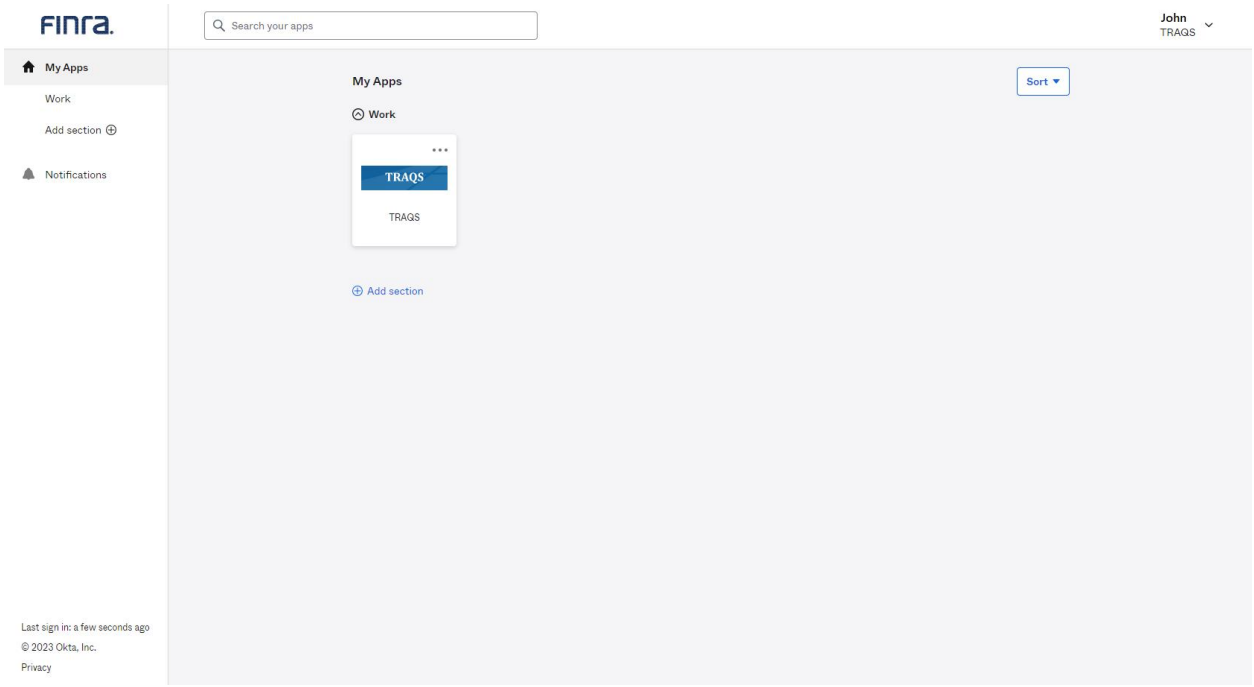


5. Once you have completed the verification set up, you will be directed back to the **Preferred Authentication Method** screen with rest of available verification choices. Please continue reading for a description of each authentication method and instructions for enrollment.
6. Select **Set up later** if you are finished setting up your authentication methods. Please see How to Remove My Security Methods below for information about removing Security Methods.
7. Users can choose to add additional factors or proceed directly to the TRAQS website. Please see Section 3 below for instructions on logging into the TRAQS website using MFA.
8. The website will prompt you to use your chosen security method(s) to login.

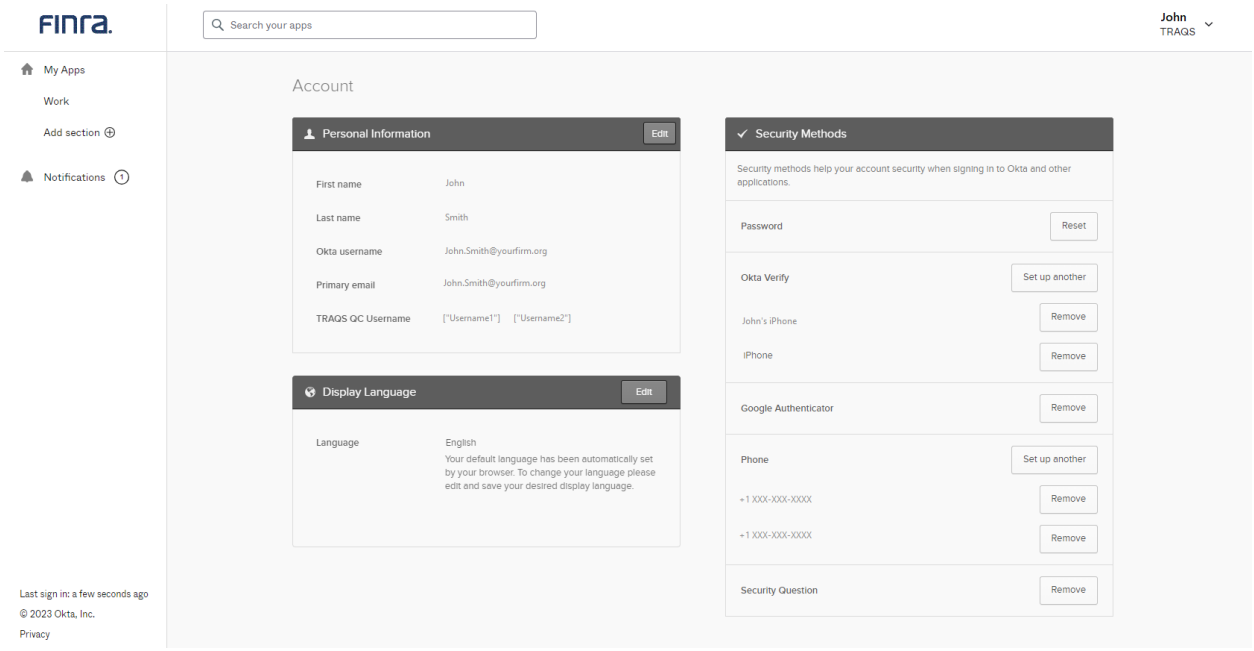
Note: The user must have access to the mobile device or land line associated with the phone number in order to login using this authentication method

Section 2: Profile Page (Okta Dashboard)

1. Visit the UAT website https://mpp-test.nasdaq.com OR Production website https://mpp.nasdaq.com
2. Enter your **Username (email address)** and **password.**
3. The Main Page (Home page) is where the link to the TRAQS Application resides.
4. The Vertical Masthead is always accessible. This is where you can find:
   - **My Apps** – Click to return to the Main Page (Home page).
   - **Notifications** – Click to view any notifications.
5. The Horizontal Masthead is always accessible. This is where you can find:
   - **FINRA Logo** – Click to return to the Main Page (Home page).
   - **User Profile** – Settings, Preferences, Recent Activity or Sign out selections:
     - User can select **Settings** to go to the Account Page
     - User can select **Preferences** where you can change the Layout or Pop up messages timer
     - Users can select **Recent Activity** where you can view the Sign-ins and Security Events information
     - User can select **Sign out** to Sign out of the Profile Page

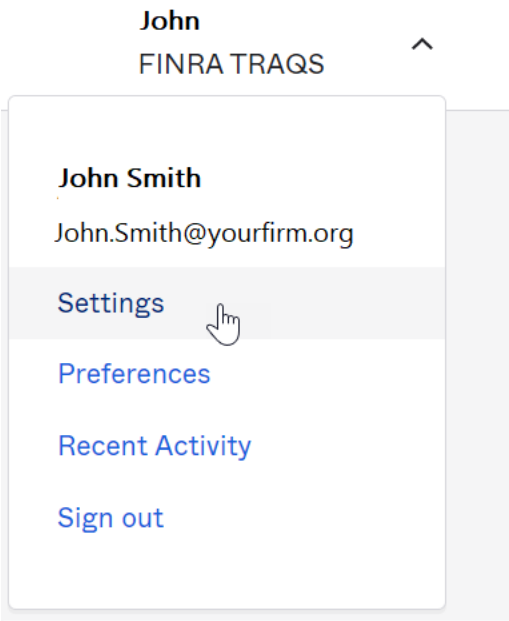


6. The Account Page is where you can view Personal Information, Reset Password, Remove Security Question, Setup/Remove Security Methods, and Change Display Language. Click on your **Name** and select **Settings.** This will open the Account page.

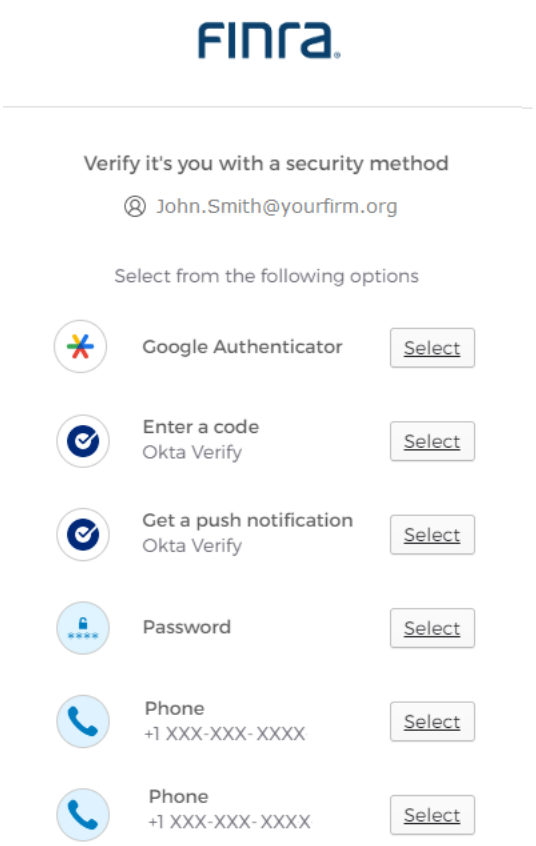


How to Edit the User Profile

1. Visit the UAT website https://mpp-test.nasdaq.com OR Production website https://mpp.nasdaq.com.
2. Enter your **Username (email address)** and **password.**
3. Click on your **Name** and select **Settings.** This will open the Account page.



4. Authenticate your account using your chosen authentication method(s). Select the method you wish to use. The screen only contains authentication methods that you have enrolled in.

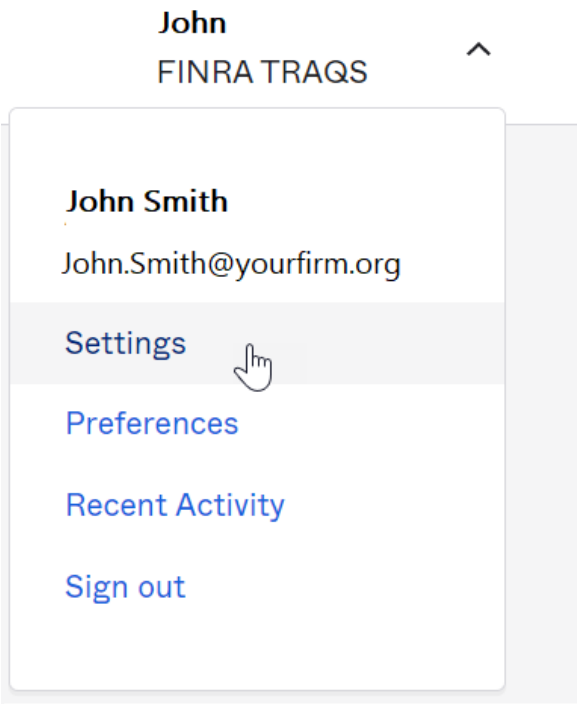


5. Users are able to update the information in the profile screen by clicking the **Edit** button beside the profile item. **Note:** Security Methods will not have the edit button.
6. Users can not edit the personal information section of this site. If your primary email or phone number need updating, please contact **FINRA Market Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.**
7. To **Reset your Password:** Click on reset, a popup asking "Are you sure you want to reset Password enrollment?" will come up, click **Yes**. Verify with a security method and password, when the new screen comes up, enter a New password and Re-enter the new password. If you want to sign out of all devices (all Okta Dashboards) click the Sign me out of all other devices checkbox. If your password was changed you will be directed back to the Profile screen and a popup saying "Sucessfully reset your password."
8. To **Remove a Security Methods(s)**: See the next section in this document "How to Remove My Security Methods" for instructions.
9. To **Set up a Security Methods(s)**: Click **Setup** next to the security method and follow the prompts OR review the appropriate set up instructions in Section 1 of this document.
10. To **Remove your Security Question:** Click the Remove button, a popup asking "Are you sure you want to remove Security Question enrollment?" will come up, click Yes and Verify with your Password and Factor. If your security question was removed you will be directed back to the Profile screen and a popup saying "You have successfully removed your security question". To add a Security Question back click the Setup button and follow the promtps.
11. To **Change the Display Language** of the profile screen: click on the edit button and select the language you prefer from the drop down, click Save.

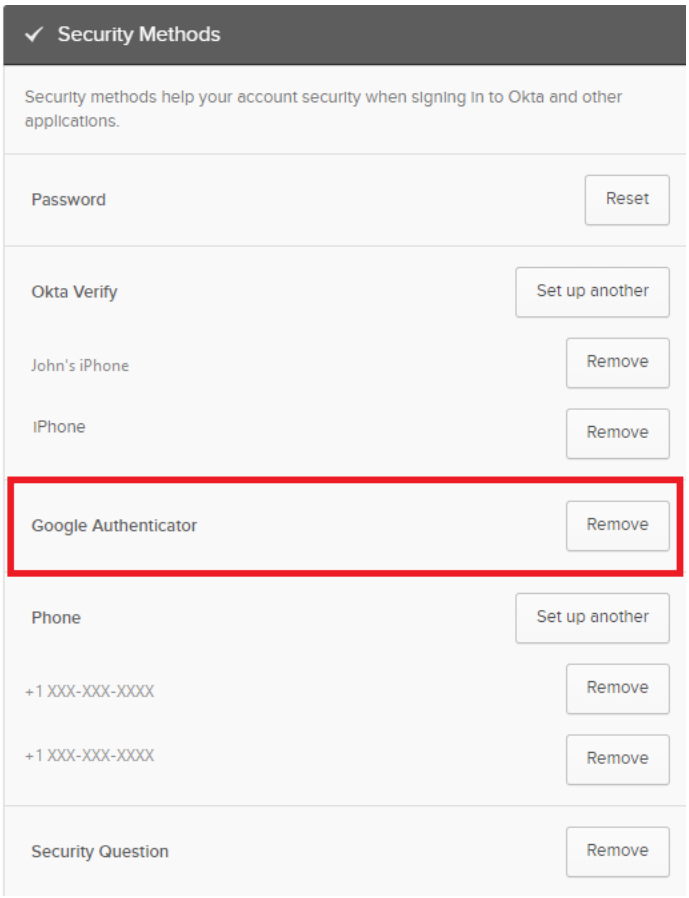
Note: If you Change the Security Methods (including a Security Question) you will receive an email from Okta notifying you of the change.

How to Remove My Security Methods

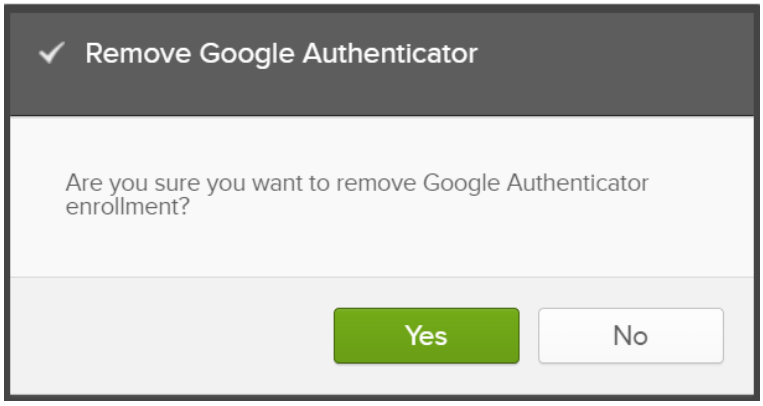
1. Visit the UAT website https://mpp-test.nasdaq.com OR Production website https://mpp.nasdaq.com.
2. Enter your **Username (email address),** click **Next.**
3. Enter your **password,** click **Verify.**
4. Authenticate your account using your chosen authentication method(s). If you have more than one method the last one you used will come up automatically.
5. If you want to use another method, click the "Verify with something else" link at the bottom of the screen. The screen will only contain authentication methods you are enrolled in.
6. Click on your **Name** and select **Settings.** This will open the Account page.



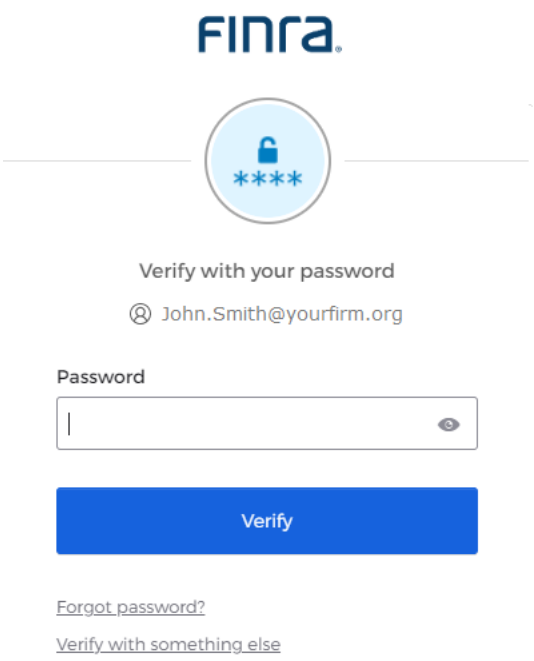
7. Under the Security Methods menu click the **Remove** button beside the authentication method. **Note:** In the following example we are removing Google Authenticator.



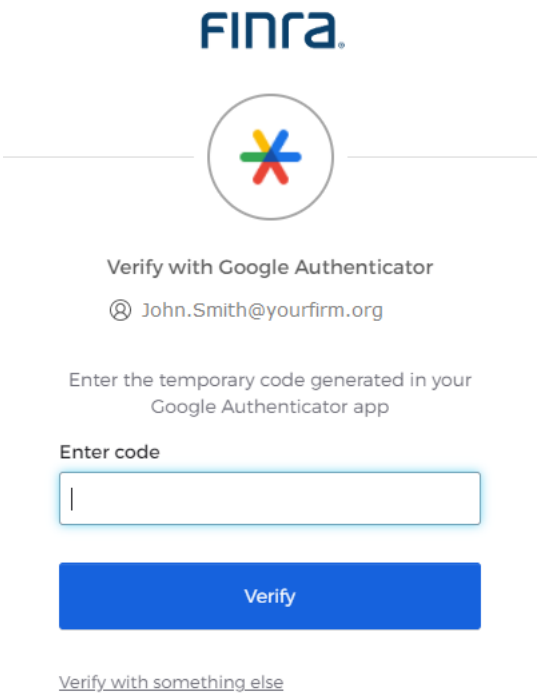
8. Confirm that you want to remove the authentication method by clicking the **Yes** button.



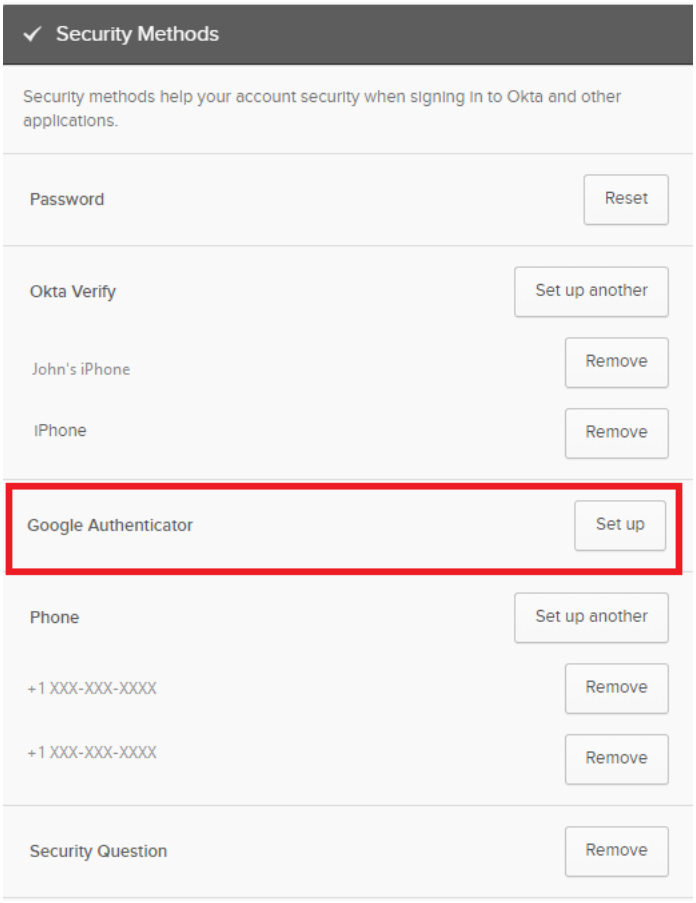
9. Enter password, click **Verify**.



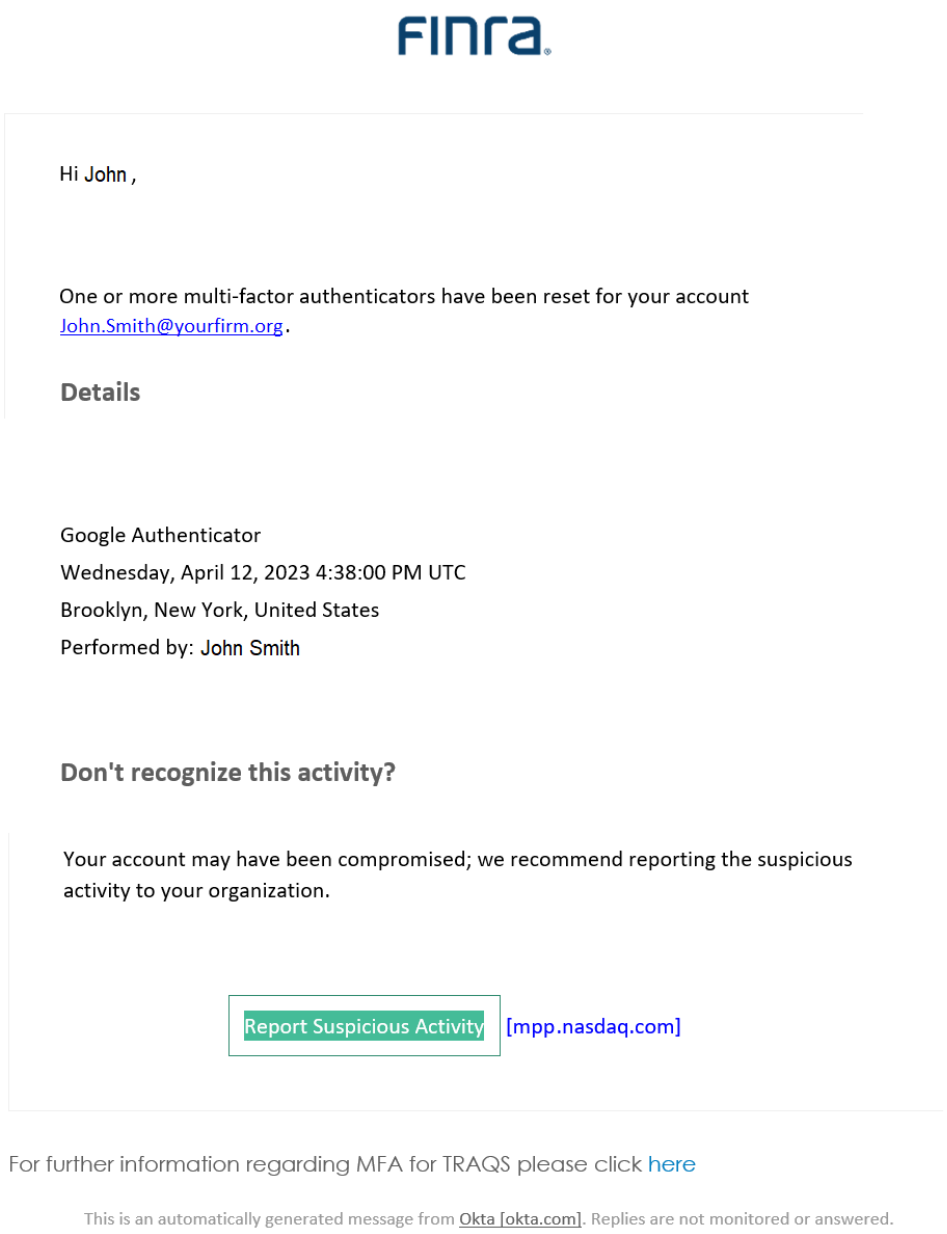
10. Verify with Factor.



11. Once Verified you will be directed back to the profile page a popup saying “You have successfully removed Google Authentication” and the Google Authentication button will now say “Set up.”



12. You will receive an email alerting you that an authentication method has been reset.



FINRA

Hi John ,

One or more multi-factor authenticators have been reset for your account John.Smith@yourfirm.org.

Details

Google Authenticator
Wednesday, April 12, 2023 4:38:00 PM UTC
Brooklyn, New York, United States
Performed by: John Smith

Don't recognize this activity?

Your account may have been compromised; we recommend reporting the suspicious activity to your organization.

Report Suspicious Activity [mpp.nasdaq.com]

For further information regarding MFA for TRAQS please click here

This is an automatically generated message from Okta [okta.com]. Replies are not monitored or answered.

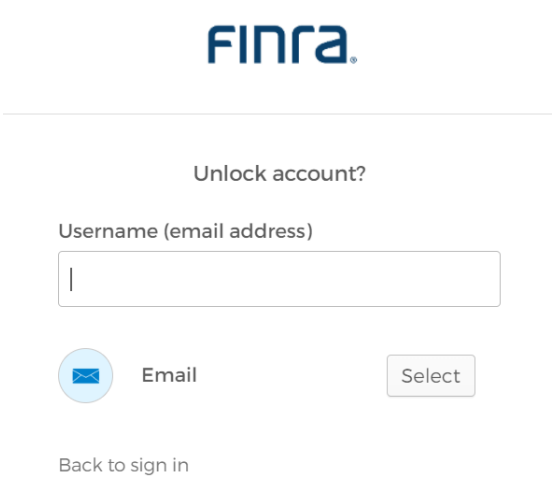
Note: You must have at least one security method set up in order to access the TRAQS website.

How to Unlock your Account

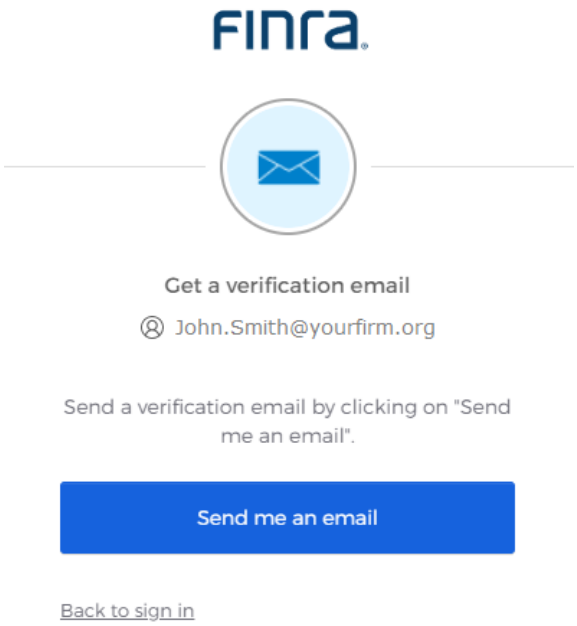
If you enter your password or authentication credentials inaccurately too many times your account will lock. The account will automatically unlock after 15 minutes.

The user will also receive an **Account Locked** email with instructions for unlocking the account. Please follow the steps below to unlock your account.

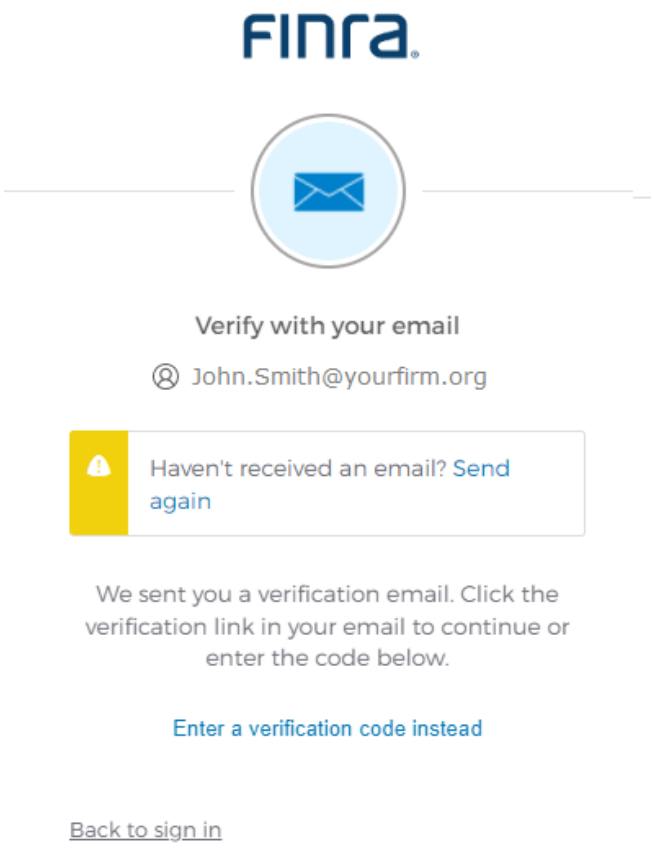
1. Enter Username (email address), Click **Select.**



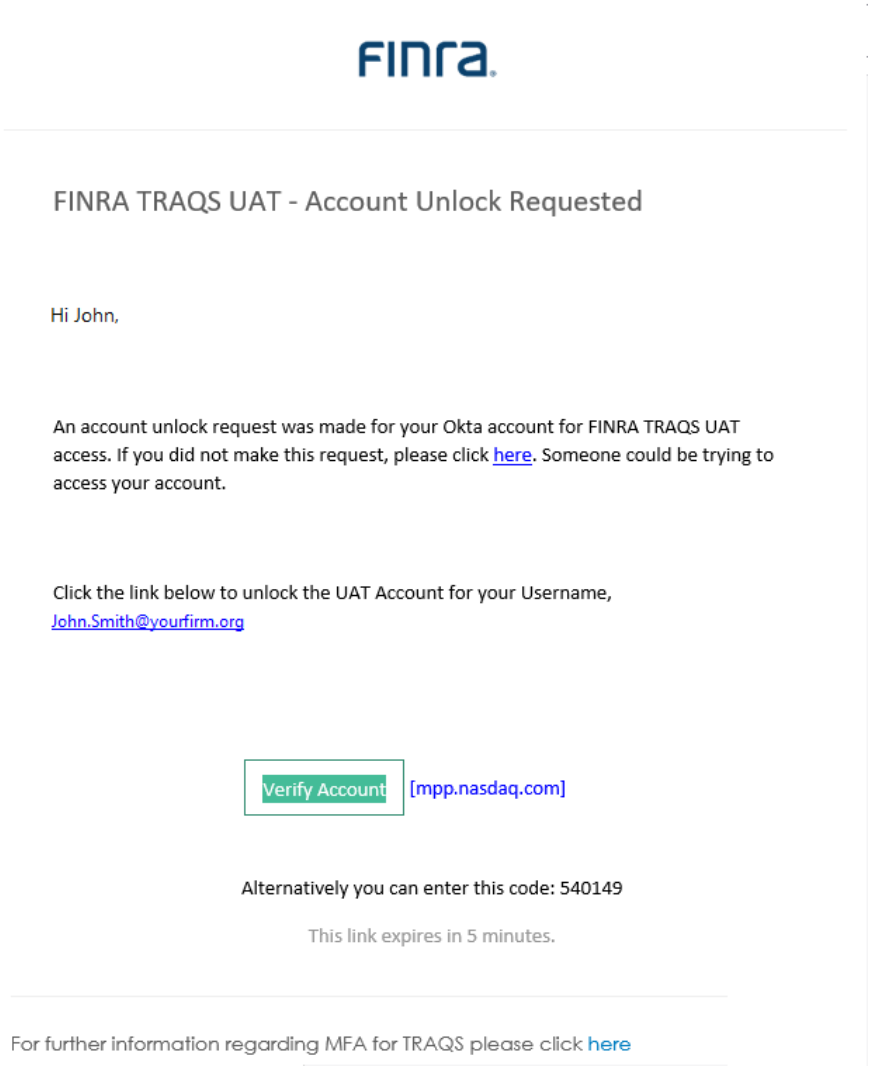
2. Click **Send me an email.**



3. A **Verification link** will be sent to your email.



4. Click the **Verify Account** link in the email -OR- **Enter the Code,** click **Verify.**



FINRA

FINRA TRAQS UAT - Account Unlock Requested

Hi John,

An account unlock request was made for your Okta account for FINRA TRAQS UAT access. If you did not make this request, please click here. Someone could be trying to access your account.

Click the link below to unlock the UAT Account for your Username, John.Smith@yourfirm.org

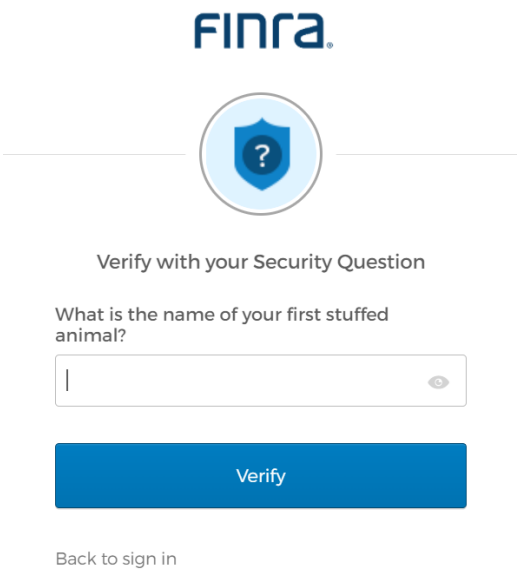
Verify Account [mpp.nasdaq.com]

Alternatively you can enter this code: 540149

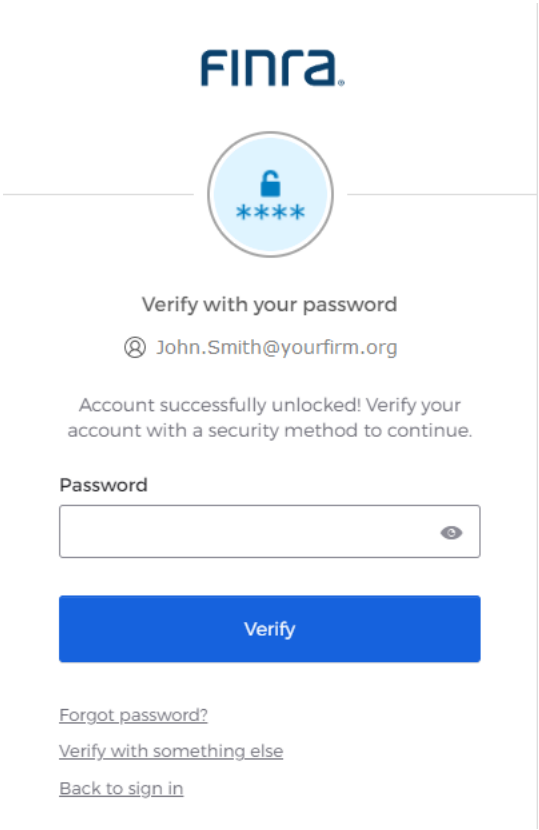
This link expires in 5 minutes.

For further information regarding MFA for TRAQS please click here

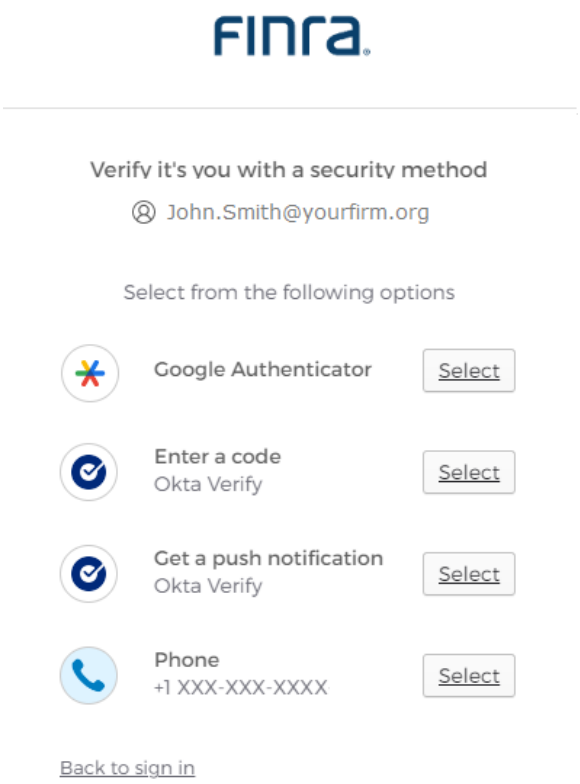
5. Answer the **Your Security Question,** click **Verify.**



6. Enter your **password,** click **Verify.**



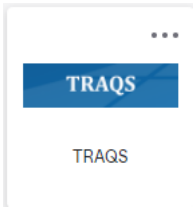
7. Click **Select** next to one of your chosen authentication methods(s).



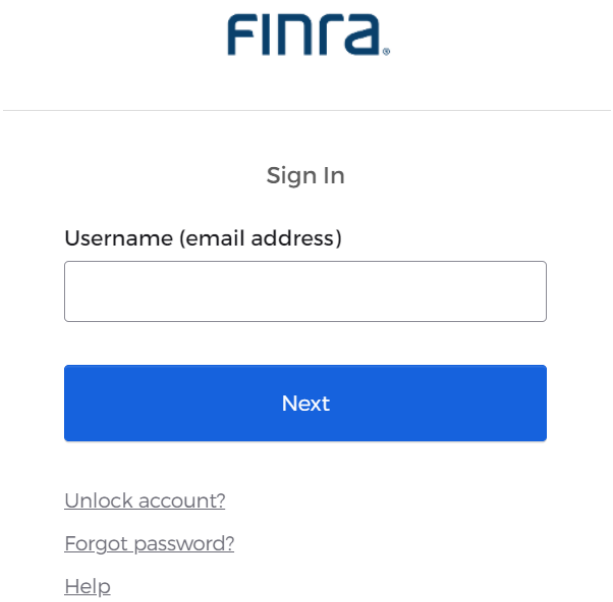
Note: Your account automatically unlocks after 15 minutes. If you do not act on the unlock email within 15 minutes your account will automatically unlock.

Section 3: How to Login to the TRAQS Website Using MFA

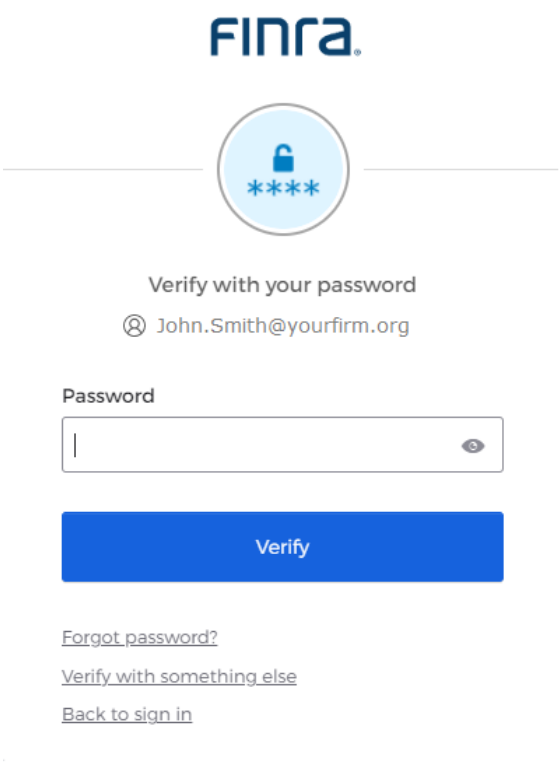
1. Enter the TRAQS URL in your browser **OR** from the Main Page (Home page) click on the TRAQS website icon in your Profile page. **Note:** If you access TRAQS thru the profile page you will not have to enter your factor again.



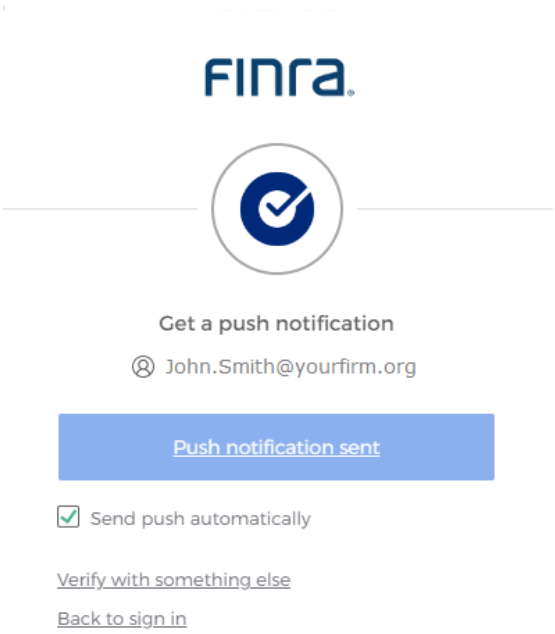
2. Enter your **Username (email address),** click **Next.**



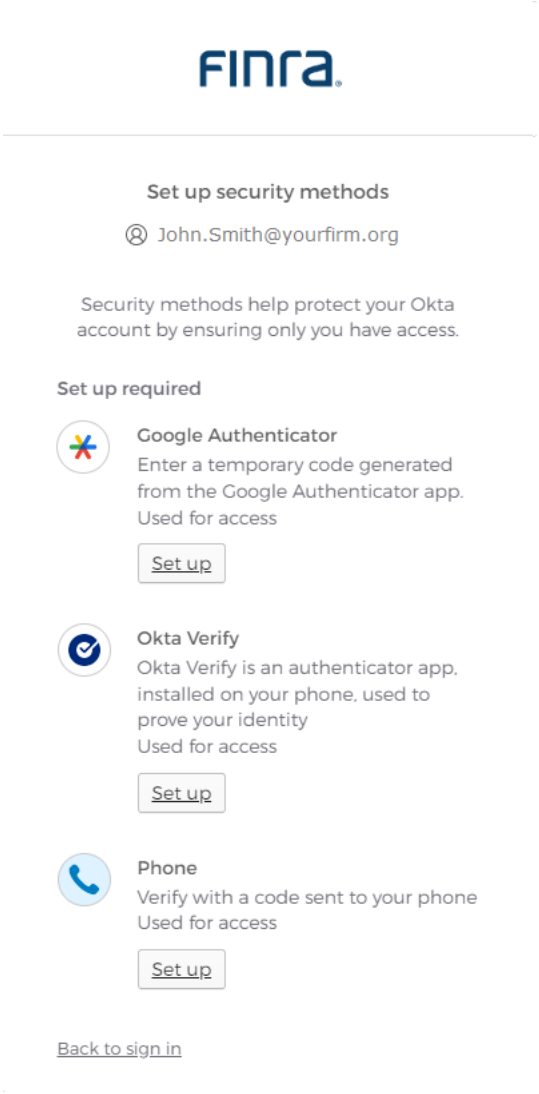
3. Enter your **Password,** click **Verify.**



4. The system defaults to the last used security method to log you in. (In the following example we are using Okta Verify (push notification)). **Note:** If you want to login with a different security method, click the **Verify with something else** link and click **Select** next to one of your chosen authentication methods. The screen only contains authentication methods that are enrolled in.

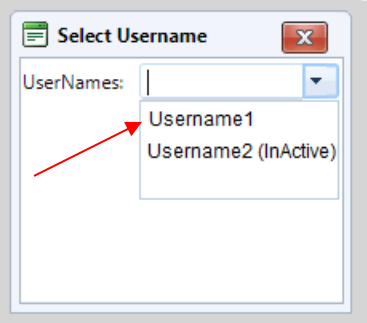


4a. If you did not set up an Authentication Method your screen will look like this. Set up an Authentication. Complete the steps outlined in Section 1 of this document to set up a new authentication method.



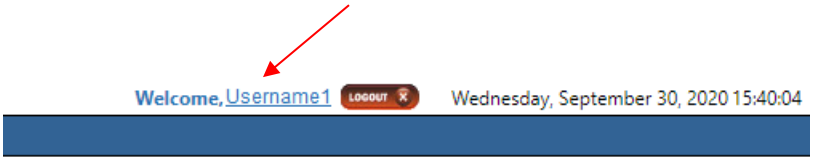
5. **If a user has only one username associated with their Username (email address),** users will be directed into the TRAQS website.

6. **If a user has multiple usernames associated with their Login (email address),** there will be several available options in the drop-down list of usernames. Choose the **Username** you want to use and click the **Select** button

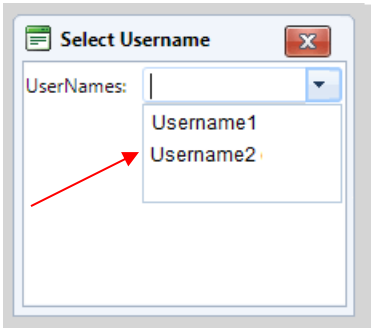


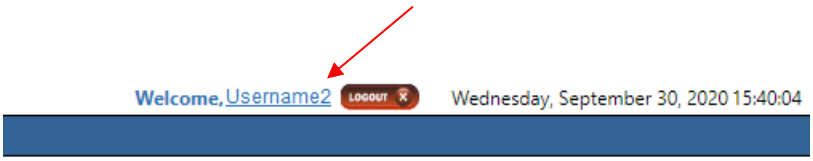
Note: If your username in the drop down above has "InActive" beside it. Please contact your Super Account Administrator and have them reset your account to active in PDM.

7. You will now be using the credentials from the username you selected.
8. To switch to different Username. Click the **Username** link found at the top right corner of TRAQS screen.



Popup screen will come up, select a **Different Username,** click the **Select** button and you will see the username change.



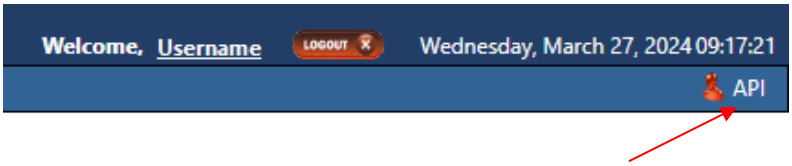


Section 4: How to Access the API Download (Manual)

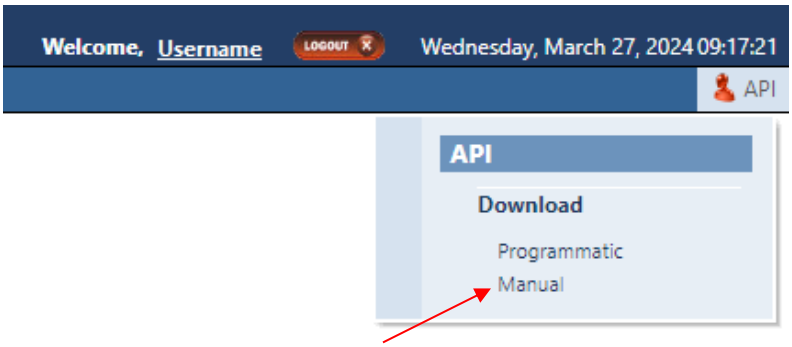
Users with API access are required to complete the steps outlined in Section 1 of this document prior to downloading the API files via web. Please see the individual FINRA product API Specification document for the specific facility to learn more about the individual files.

To successfully download the files Manually, your Okta password must not be expired, your TRAQS login must be active, and you are authorized for API.

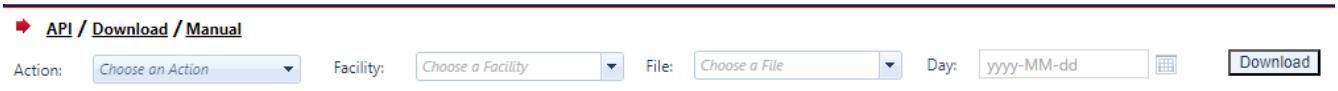
1. Login to TRAQS using MFA as outlined in Section 3 of this document.
2. Click **API** from the **Main Menu**.



3. Click **Manual** from the **Download Menu**.



4. Choose the **Action**, **Facility**, **File** and **Day** (if applicable) from the **API Download Manual screen**.



Action:

- Download – Downloads the complete file.
- Delta – Used for Daily List requests. Downloads the changes since the last time the user download the file.

Facility:

- TRACE – CA
- TRACE – SP
- TRACE – TS
- ADF
- ORF

Note: Users must have authorization to the specific facility in order to successfully download a file.

File:

Note: Please reference the API Specification for the facility to learn more about what files are available.

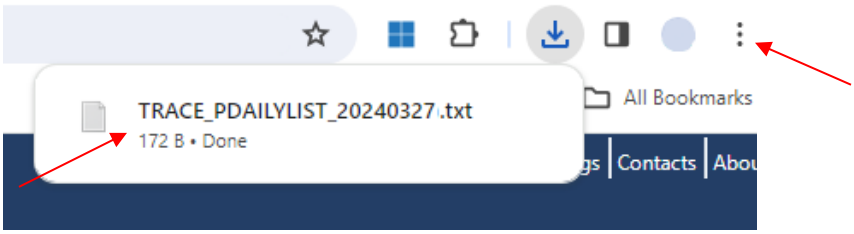
Day:

Note: Day is used for Daily List requests with Action of "Download" only. Day will not be available for Daily List requests with an Action of "Delta."

5. Click **Download**. Messages will be generated to show that the request was sent and completed.

   - DOWNLOAD REQUEST SENT...
   - DOWNLOAD COMPLETE.

6. Click on the **popup** to open the downloaded file.



Note: If the download icon and file does not automatically popup (see screen above), click on the three dots or three lines (depending on your browser) in the top right corner to expand the menu and click downloads submenu, where all your downloaded files are located.

7. The file you chose to download will open.

Note: The API Specifications can be found in the following locations:

TRACE Fixed Income - https://www.finra.org/filing-reporting/trace/documentation
ADF - https://www.finra.org/filing-reporting/adf/adf-documentation
ORF - https://www.finra.org/filing-reporting/orf/orf-forms-and-documentation

Section 5: How to Access the API Download (Programmatic)

Users with API access are required to complete the steps outlined in Section 1 of this document prior to downloading the API files. The enrollment steps outlined in Section 1 need to be completed once per user account.

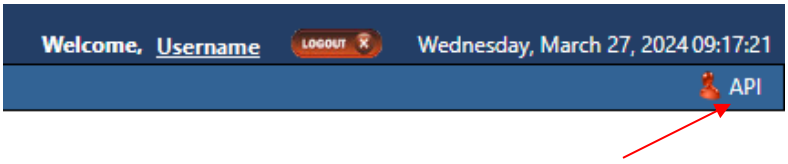
To successfully download the files Programmatically, your Refresh and Access token must not be expired, your TRAQS login must be active, and you are authorized for API.

Users who wish to programmatically access the API must request a Refresh Token via the TRAQS Website with their OKTA profile login. This Refresh Token will be used to obtain an Access Token. This Access Token will use a "Bearer Token," which will allow clients to request the API files without having to collect credentials.

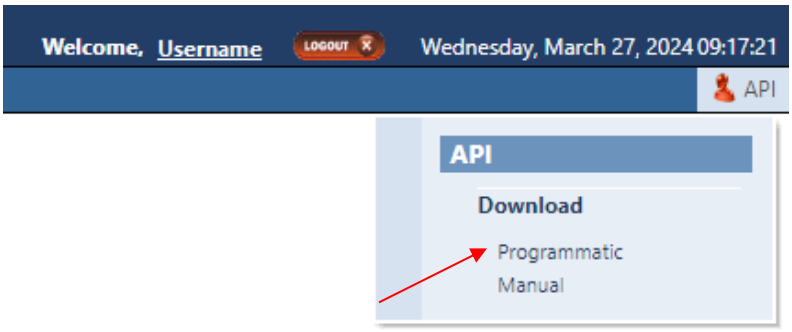
The Refresh Token is valid for 6 months. The Access Token expires every hour (3600 seconds). It is the clients responsibility to programmatically request a new Access Token when it expires using the Refresh Token.

To access TRAQS, a username, password, and NASDAQ Multi-Factor Authentication (MFA) is required. To establish a TRAQS username, please consult your Super Account Administrator (SAA) and use the Participant Data Management (PDM) system.

1. Complete the steps outlined in Section 1 for the TRAQS login.
2. Log into TRAQS and authenticate using MFA.
3. Click **API** from the **Main Menu**.

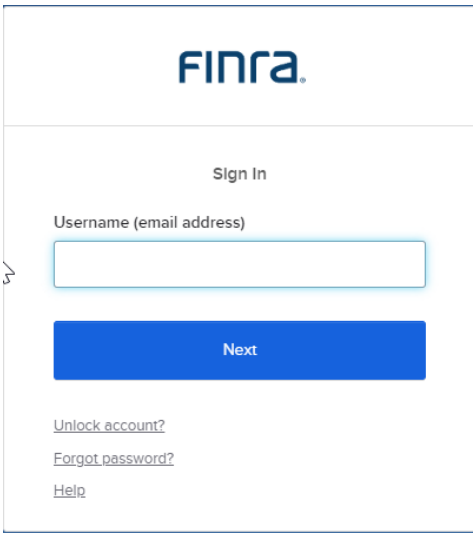


4. Click **Programmatic** from the **Download Menu** (this is where the Refresh Token is obtained).

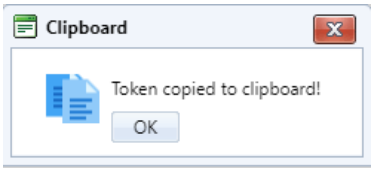


5. Click **Get Token** from the **API Download Programmatic screen**.

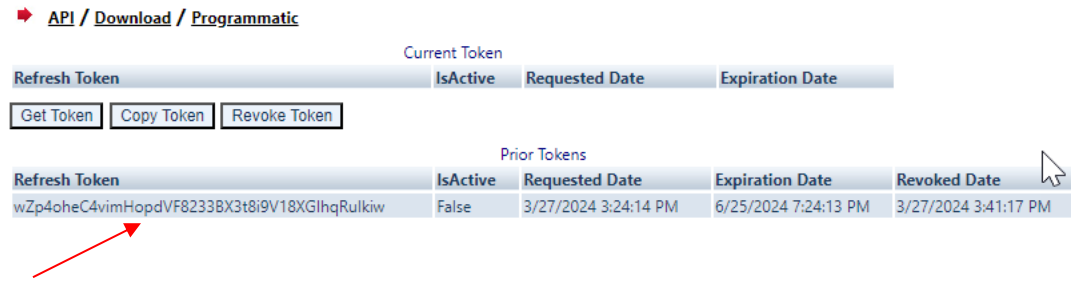
6. After requesting the Refresh Token the system will ask you to **Authenticate** again. If successful the user will be brought back to the API Download Programmatic screen and the Refresh Token information will be populated under the "Current Token" portion of the screen.



7. Click **Copy Token** and paste the **Refresh Token** into your script.



8. Add code to your script to request an **Access Token.**
9. Upon logging into the API domain from your application, your application will request a new Access Token from the TRAQS download server.
10. Your application will apply the new Access Token to the download API request call.
11. On success, the requested data will be returned to your application.
12. The user has the ability to Revoke the current Refresh Token at any time, by clicking **Revoke Token**. This will inactivate the current Refresh Token and it will move to the Prior Token portion of the screen.



13. If the current Refresh Token is expired, click **Get Token** which will generate a new Refresh token and the expired Refresh Token will move to the Prior Token portion of the screen.

Note: Users will be notified via email 15 days prior to expiration. You cannot download the API files if the **Refresh Token** or **Access Token** are expired. Your code should be written to detect an expired Access Token and re-request it programmatically after expiration. Refresh Tokens that expire will need to be requested manually following step 3 above and be updated in your script.

Section 6: Common Questions

Why is FINRA implementing Multi Factor Authentication (MFA) for TRAQS?

Passwords are increasingly easy to compromise. Passwords can often be stolen, guessed, or hacked; often without the user knowing. MFA adds a second layer of security by helping the account stay secure even if the password is compromised.

Is enrollment in MFA mandatory?

Yes, users are required to enroll in MFA to access the FINRA TRAQS website for trade reporting and API access. Any user that attempts to login to the TRAQS website without enrolling in MFA will be prompted to enroll in MFA.

It is recommended that users enroll in more than one authentication method. Voice call authentication using a phone number that differs from the phone number associated with your original authentication number is the preferred back up authentication type.

My SAA requested a new TRAQS Username for me, I have not received an enrollment email. How do I get a new email?

If you need a new enrollment email, please contact finraoperations@finra.org or 1-866-776-0800 option 2.

Does the enrollment email expire?

Yes. Users have 30 days from the date the email was sent to take action to set up the Okta account for TRAQS access Username (email address). If your enrollment email expired, please contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.

What do I do if I lost my mobile device?

It is strongly recommended that you remove the lost device from your MFA settings. Enter the Okta profile screen and remove the authentication method associated with the device. Please see Section 2 for instructions.

If your enrolled device is lost and you have not enrolled in any additional methods of authentication using alternative devices, please contact NASDAQ tech support at 212-231-5180.

Why do I have 2 Okta verify or 2 Google Authentication accounts?

The NTF (UAT) and production environment for TRAQS are separate. The account https://mpp-test.nasdaq.com is associated with NTF (UAT) access. The account https://mpp.nasdaq.com is associated with production access.

How can I edit my personal profile data?

Your profile data can be edited at any time. Please see Section 2 for instructions. Please note, the personal information section of the user profile cannot be edited. Please have your SAA contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org to update this data.

Can I set up a push notification when using Okta Verify?

Yes, users can select the "send push automatically" at any time after enrolling in Okta verify. Be sure to turn on notifications, on your device. Your device will receive a notification asking to approve the login. Once you select approve you will be directed to the TRAQS website as normal.

Why did I receive two MFA enrollment emails from Okta?

You received two enrollment emails because you are set up to access TRAQS in both the production and test environment. Although your Username may be the same for both environments, they require two separate enrollments. Please follow the How to Enroll and Choose Authentication Method instructions above for each environment.

I have forgotten my password or entered my authentication method inaccurately a few times and locked my account. How can I unlock it?

Your account will automatically unlock after 15 minutes. There are two ways to unlock your account.

1. You will receive an email notifying you that your account is locked. Follow the instructions in the email to unlock your account.

2. Click the "Forgot password" OR "Unlock account" link at the bottom of the TRAQS Sign In screen. Enter your email address in the provided box to generate a reset email. Click on the Reset Password -OR- Unlock Account link in the email within the 8-hour expiration and answer your forgotten password questions.

If you do not know the answers to any of your forgotten password options, need assistance with unlocking your account or any other password issues, you may call NASDAQ tech support at 212-231-5180 option 4.

Why am I also receiving an email for a TRAQS certificate if I have enrolled in MFA?

Until NWSF certificates are eliminated, users will receive an email for MFA enrollment and a TRAQS NWSF certificate. Users who have access to API will use the NWSF certificate and password to access API files. Only users with API privileges will be able to access the API files using the TRAQS certificate.

What is the Okta Dashboard (profile link) to the test environment?

Users can enroll, edit their profile and log into TRAQS in the test environment using the following link https://mpp-test.nasdaq.com

What is the Okta Dashboard (profile link) to the production environment?

Users can enroll, edit their profile and log into TRAQS in the production environment using the following link https://mpp.nasdaq.com

I am an API user and would like to Manually access the API. How do I access the files?

Users can access the API files by logging into TRAQS, selecting Manual under the API menu. Please see the User guide for the specific facility for more information.

I am an API user and want to access the API in an Automated fashion. How do I access the files?

Users can access the API files by logging into TRAQS to get a Refresh Token to use in your code. The Refresh Token is located in the Programmatic window under the API menu. Please see the API user guide for the specific facility for more information.

Can I have more than 1 Access Token at a time for the Programmatic API download?

Yes. You can download the file from more than one machine as long as the Refresh Token and Access Token are still valid.

How long do Refresh Tokens and Access Tokens for Programmatic API downloads remain valid?

A Refresh Token remains valid for 6 months from the date of issue. The account owner will receive an email 15 days prior reminding the user of expiration. Users must login to TRAQS and confirm their identity using their second authentication method to obtain a new Refresh Token per the instructions in Section 5.

The Access Token expires every sixty (60) minutes. Systems will need to be programmed to detect an expired Access Token and request a new one programmatically after expiration.

If you are having issues logging into the TRAQS website, please contact FINRA Operations at 1-866-776-0800.

Can I automate the process to get a Refresh Token?

No, Every 6 months the user must login to TRAQS, confirm their identity using their second authentication method to obtain a new Refresh Token per the instructions in Section 5

What if the Refresh Token is expiring and the primary account owner is unavailable and cannot obtain a new Refresh Token?

FINRA recommends that multiple users at your firm have API access for resilience. In this instance another user with API access can login to TRAQS, confirm their identity using their second authentication method to obtain a new Refresh Token.

The account we use to programmatically pull API files is a generic account. What MFA method should we use to enroll?

FINRA recommends enrolling in voice call authentication using a general phone number. FINRA also encourages phone authentication as a backup authentication method. **Note:** the same type of authentication method can be set up multiple times. I.e., in this instance the account can have multiple landlines set up.

400 Error

If you receive a 400 Error = 400 (400 = Bad request). The API request is most likely incomplete. Please follow the details outlined in the relevant API Specification in the Requesting an Access Token section to ensure the request includes all necessary data.

What is the new test environment URL to Access the API Download Programmatically?

The new URL is https://apidownload-ntf.finratraqs.org.

What is the new production environment URL to Access the API Download Programmatically?

The new URL is https://apidownload.finratraqs.org.

403/404 Errors

If you receive a 403 App not assigned or 404 Page not Found error contact NASDAQ tech support at 212-231-5180 option 4.

Report Suspicious Activity

To report unrecognized activity from an account activity email notification. Contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.

Okta Account Token Expiration Error

If your Account Activation Token is no longer valid. Contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.

Need Help?

If you need assistance using Multi Factor Authentication for TRAQS, contact the FINRA Market Operations at 1-866-776-0800 option 2.

Section 7: Revision History

Date	Version	Changes
11/12/2020	1.0	Initial Version
02/16/2021	1.1	Updated document to include information relevant for production release. Updates are as follows: • **Section 2: Profile Page** - Included links to the production site • **Section 4: How to Access the API Download** - Included production parallel • **Section 5: Common Questions** - Included common questions regarding MFA production migration
01/31/2022	1.2	Updated document with PDM (Participant Data Management System)
10/30/2023	1.3	Updated document to include a slight change in the sign-on process and look and feel • Remembers the user's last-used security method and displays it at the next sign-on • Users can select a different security method if they do not want to use the last-used one • Security images are not supported any longer • Voice and SMS are under Phone • No more Welcome Wizard • Can view Recent Activity in Okta Dashboard When setting up new user, you need to enroll in both authentication and recovery factors
04/24/2024	2.0	Updated document to include information relevant for production release. Updates are as follows: • **Section 4: How to Access API Download (Manual)** • **Section 5: How to Access API Download (Programmatic)** • **Section 6: Common Questions**