

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

MARCH 16, 2026 – VERSION 2.3

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

On **December 31, 2025**, FINRA retired two (2) Multi-Factor Authentication (MFA) options (SMS Authentication and Voice Call Authentication) that firms used to access the TRAQS Website, Reference API data (Manually via TRAQS and Programmatically) and replaced them with two (2) new methods;

1. Okta Verify Desktop (FastPass using features such as Windows Hello)
2. Federated Single Sign-on (SSO)

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, desktop or Federated Single Sign-On (SSO). Sharing account credentials is not recommended.

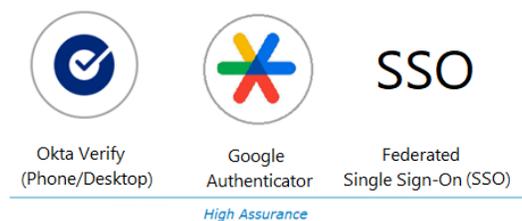
The following enrollment steps only need to be completed once per user account. For more information about MFA please see our [TRAQS MFA website](#).

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 unless stated otherwise in the document.

The available second factor authentication methods include:

1. **Okta Verify** (Mobile and Desktop(FastPass using features such as Windows Hello))
2. **Google Authenticator**
3. **Federated Single Sign-On (SSO)**

Note: Users logging in through Federated SSO no longer require an additional MFA, as the customer's identity provider (IDP) performs secure 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.. | 4 |
| Google Authenticator | 10 |
| Setting up Google Authenticator | 10 |
| Okta Verify (Mobile) | 13 |
| Setting up Okta Verify | 13 |
| Okta Verify (Desktop) | 17 |
| Setting up Okta Verify FastPass..... | 17 |
| Adding an Account from Another Device | 24 |
| Use Another Account | 27 |
| Federated Single Sign-On (SSO)..... | 28 |
| Setting up Federated SSO..... | 28 |
| Section 2: Profile Page (Okta Dashboard)..... | 29 |
| How to Edit the User Profile | 31 |
| How to Add a Security Method(s) | 33 |
| How to Remove a Security Method(s) | 35 |
| How to Unlock your Account..... | 40 |
| Section 3: How to Login to the TRAQS Website Using MFA..... | 45 |
| Section 4: How to Access the API Download (Manual) | 50 |
| Section 5: How to Access the API Download (Programmatic)..... | 53 |
| Section 6: Common Questions | 57 |
| Section 7: Revision History..... | 61 |

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**.



FINRA TRAQS - Welcome to Okta!

Hi John,

FINRA is using Okta to manage the Multi-Factor Authentication for TRAQS.

An Okta account for FINRA TRAQS access has been created for you.
Click the link below to activate your Okta account:

Activate Okta Account [\[mpp.nasdaq.com\]](https://mpp.nasdaq.com)

This link expires in 30 days.

Your Username (email address) is John.Smith@yourfirm.org
FINRA's Okta Account for TRAQS access sign-in page is
<https://mpp.nasdaq.com> [\[mpp.nasdaq.com\]](https://mpp.nasdaq.com)

For further information regarding MFA for TRAQS please click [here](#)

This is an automatically generated message from [Okta \[okta.com\]](https://okta.com). Replies are not monitored or answered.

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



Set up security methods

📧 John.Smith@yourfirm.org

Security methods help protect your FINRA TRAQS account by ensuring only you have access.

Required now

 **Password**
Choose a password for your account

[Set up](#)

 **Security Question**
Choose a security question and answer that will be used for signing in

[Set up](#)

[Back to sign in](#)

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




Set up password

📧 John.Smith@yourfirm.org

Password requirements:

- At least 12 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Does not include your first name
- Does not include your last name
- Your password cannot be any of your last 7 passwords
- At least 1 day(s) must have elapsed since you last changed your password

Enter password

Re-enter password

Next

[Return to authenticator list](#)

[Back to sign in](#)

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



Set up security methods

📧 John.Smith@yourfirm.org

Security methods help protect your FINRA TRAQS account by ensuring only you have access.

Required now



Google Authenticator

Enter a temporary code generated from the Google Authenticator app.

[Set up](#)



Okta Verify

Okta Verify is an authenticator app, installed on your phone or computer, used to prove your identity

[Set up](#)



Security Question

Choose a security question and answer that will be used for signing in

[Set up](#)

[Back to sign in](#)

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

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**.

The image displays two side-by-side screenshots of the FINRA MFA setup interface. Both screenshots feature the FINRA logo at the top and a shield icon with a question mark. The user's email address, John.Smith@yourfirm.org, is displayed below the icon.

Left Screenshot: The 'Choose a security question' option is selected. Below it, a dropdown menu is open, showing the question 'What is the food you least liked as a chi...'. The 'Answer' field is empty, and the 'Verify' button is visible at the bottom.

Right Screenshot: The 'Create my own security question' option is selected. Below it, there is an empty text input field for the user's own security question. The 'Answer' field is empty, and the 'Verify' button is visible at the bottom.

Both screenshots include links for 'Return to authenticator list' and 'Back to sign in' at the bottom.

8. Select the **Preferred Authentication Method** from the list of available choices including: [Google Authenticator](#), and **Okta Verify (Mobile or Desktop)**. [Federated Single Sign-On \(SSO\)](#) will not be an available choice under the preferred Authentication Methods list and will require additional information in order to be set up. Please continue reading for a description of each authentication method and instructions for enrollment. **Note:** FINRA recommends users enroll in more than one authentication method. Enrolling in more than one authentication method ensures continued access through redundancy.



Set up security methods

 John.Smith@yourfirm.org

Security methods help protect your FINRA TRAQS account by ensuring only you have access.

Required now



Google Authenticator

Enter a temporary code generated from the Google Authenticator app.

[Set up](#)



Okta Verify

Okta Verify is an authenticator app, installed on your phone or computer, used to prove your identity

[Set up](#)

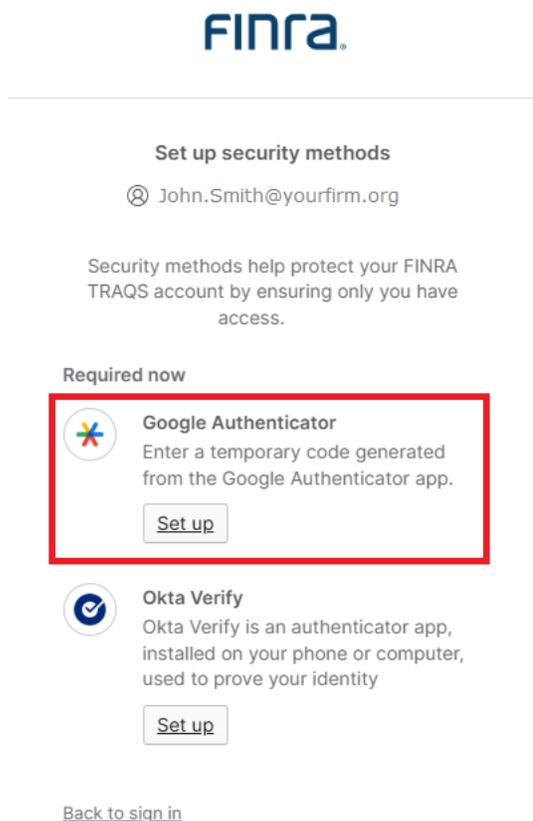
[Back to sign in](#)

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. **Note:** You can only have one Google Authenticator Security Method configured for your Okta account.

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**.



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

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**.

FINRA



Set up Google Authenticator

@ John.Smith@yourfirm.org

Scan barcode

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".



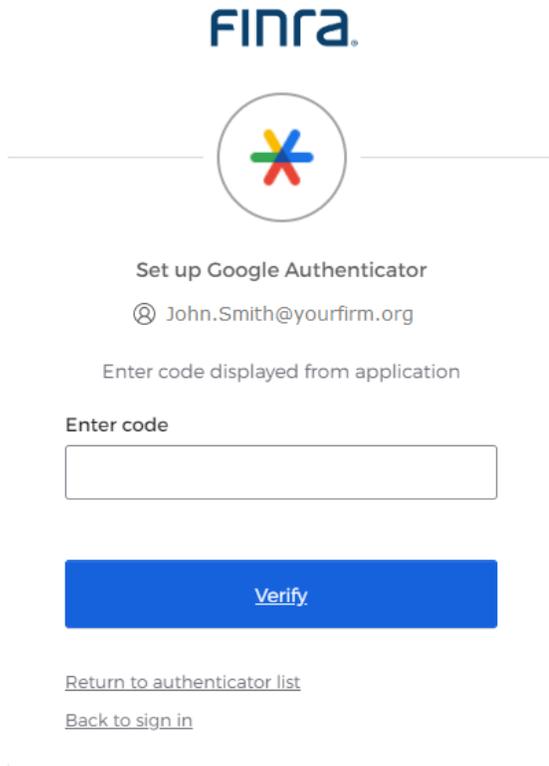
[Can't scan?](#)

[Next](#)

[Return to authenticator list](#)

[Back to sign in](#)

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.



FINRA

Set up Google Authenticator

John.Smith@yourfirm.org

Enter code displayed from application

Enter code

Verify

[Return to authenticator list](#)

[Back to sign in](#)

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 **Continue** 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.

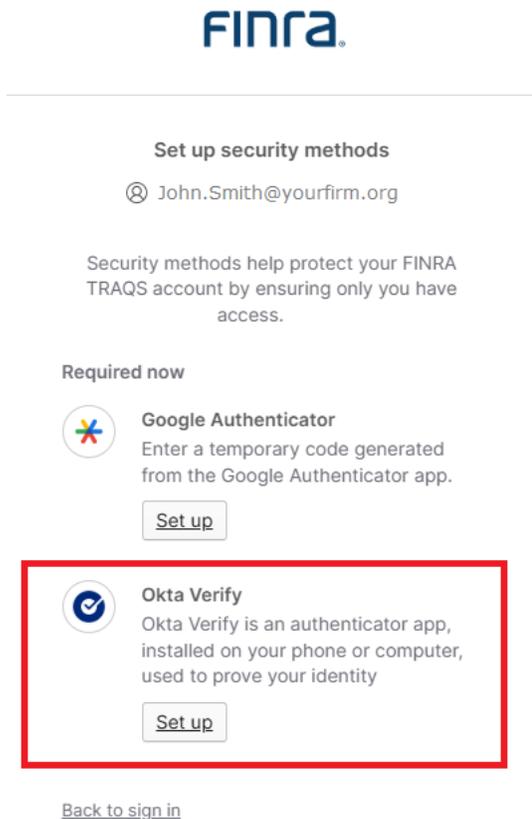
Okta Verify (Mobile)

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:** You can have multiple Okta Verify Security Methods configured for your Okta account.

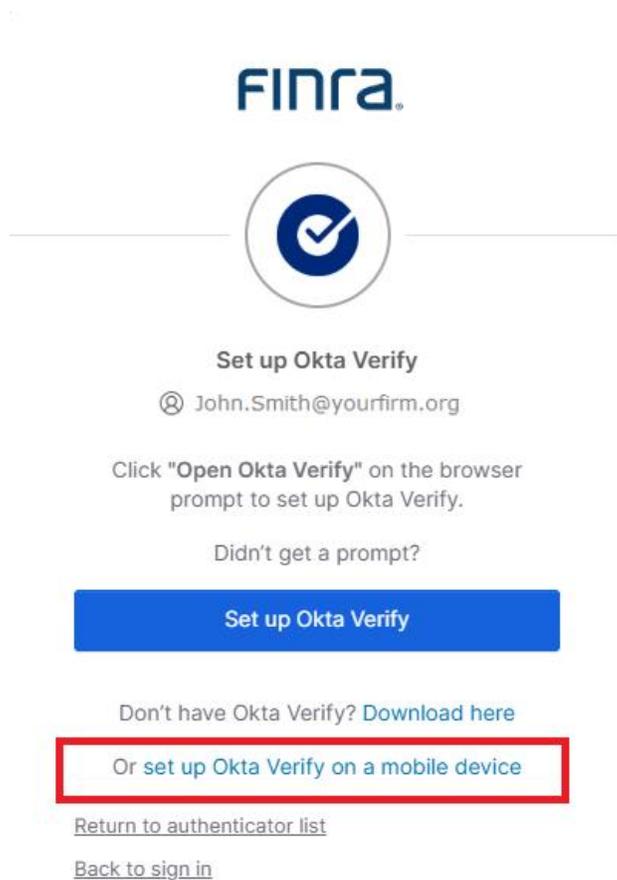
Note for iPhone users: If you would like to use Okta verify, you must have face id/touch id (iPhone 5 and higher) enabled on your phone. If you do not want to enable face id/touch id please use another verification. Also you must be on the latest iOS.

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. Click **set up Okta Verify on mobile device**.



4. A **QR Code** will appear on your computer monitor.
5. **Open** the **Okta Verify App** on your mobile device and follow instructions to add FINRA's MFA.
6. **Scan** the **Barcode** using the **Okta Verify App**.
Note: If you cannot set up Okta Verify via the QR code you can click **try a different way** which allows the user to set up Okta Verify via email or text.

FINRA



Set up Okta Verify

📧 John.Smith@yourfirm.org

1. On your other device, download the Okta Verify app from the App Store® (iPhone® and iPad®) or on Google Play (Android® devices).
2. Open the app and follow the instructions to add your account
3. When prompted, tap **Scan a QR code**, then scan the QR code below:



Or [try a different way](#) to set up Okta Verify.

[Return to authenticator list](#)

[Back to sign in](#)

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 **Continue** if you are finished setting up your authentication methods. Please see [How to Remove My Security Methods](#) below 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](#) below 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.

Enrolling in Multi Factor Authentication (MFA) to Access TRAQ5 Website and API

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

| | |
|--|--|
| <p>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.</p> | <p>Push: Access the Okta Verify app on the associated device and approve the request.</p> |
|--|--|



Verify it's you with a security method

John.Smith@yourfirm.org

Select from the following options



Enter a code
Okta Verify

Select



Get a push notification
Okta Verify

Select

Okta Verify (Desktop)

Okta Verify Desktop is an authentication application that enhances the security of accessing apps protected by Okta. Okta Verify Desktop allows users to verify your identity on your Windows computer, acting as a second factor for authentication, especially when accessing apps through Okta FastPass. This feature enables password-less or more convenient authentication experiences by utilizing the device's biometrics (e.g., Windows Hello). **Note:** You can have multiple Okta Verify Security Methods configured for your Okta account.

Setting up Okta Verify FastPass

1. Under **Okta Verify**, click **Set up**.

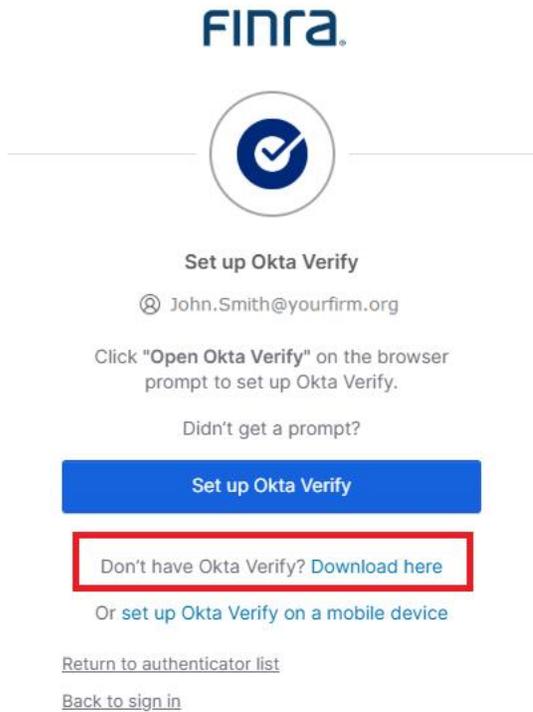
Note: If you are already enrolled with another MFA, at the FINRA TRAQS Login screen, click **Sign in with Okta FastPass**, and continue to the next step.

The image displays two screenshots from the FINRA login interface. The left screenshot, titled "Set up security methods", shows the user's email address "John.Smith@yourfirm.org" and a list of required security methods. Two methods are listed: "Google Authenticator" and "Okta Verify". The "Okta Verify" method is highlighted with a red rectangular box. Below the "Okta Verify" entry is a "Set up" button. At the bottom of the screen is a "Back to sign in" link. The right screenshot, titled "Sign In", shows a "Sign in with Okta FastPass" button highlighted with a red rectangular box. Below this button is an "OR" separator, followed by a "Username (email address)" input field and a blue "Next" button. At the bottom of the screen are three links: "Unlock account?", "Forgot password?", and "Help".

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

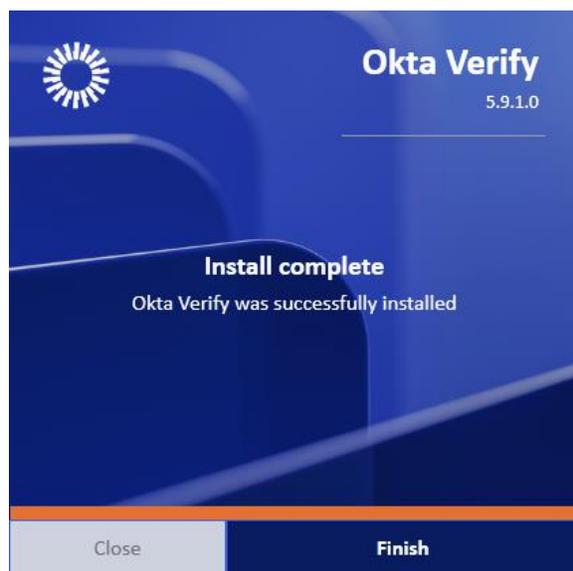
2. Click **Download here** link.

Note: Users might need administrator rights to download Okta Verify Desktop, please contact your firm's desktop support if you incur any issues.



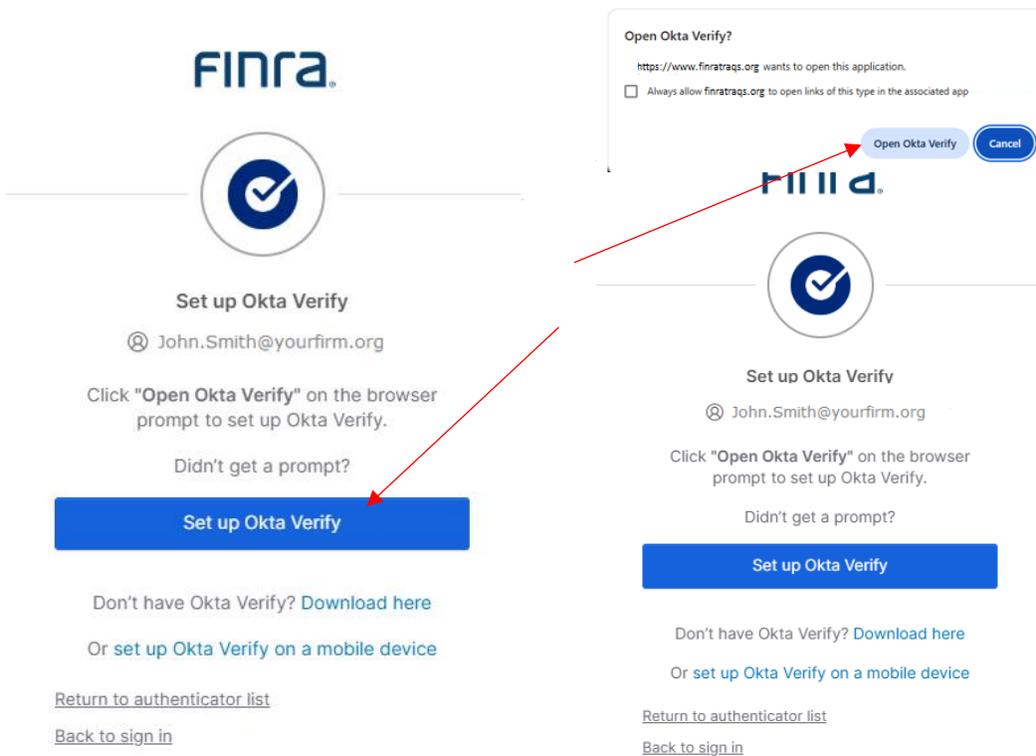
3. Select **I agree to the License and terms and conditions** checkbox, then click **Install**. Okta Verify will install to your computer. Once the install is complete click **Finish**.

Note: Users may need to work with your firm's desktop support team if you incur any issues with the install.

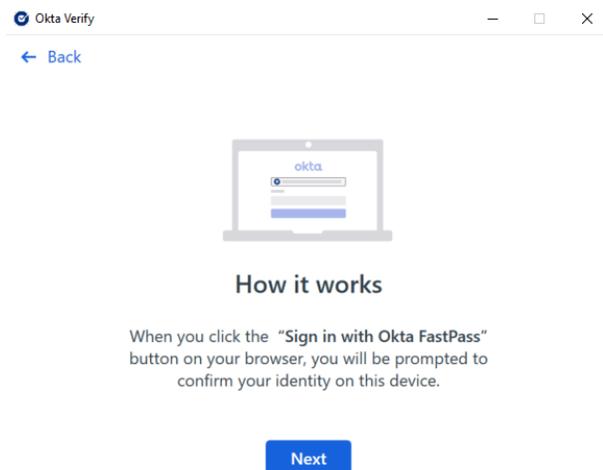
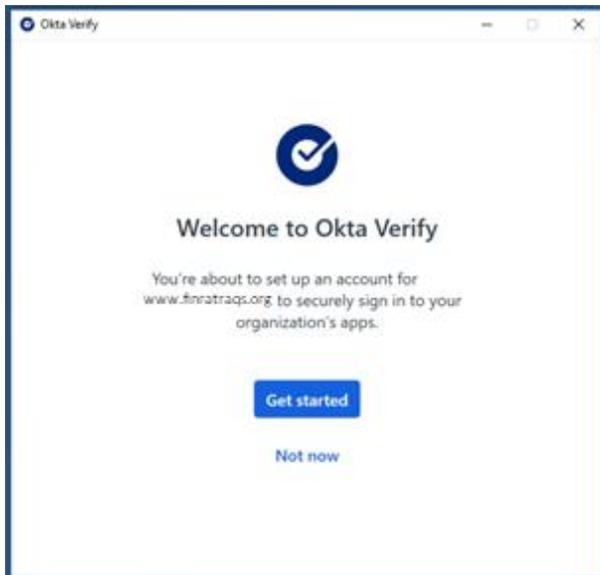


Enrolling in Multi Factor Authentication (MFA) to Access TRAQS Website and API

4. If Okta Verify doesn't open automatically, click **Set up Okta Verify**. If you get a popup click **Open Okta Verify**.



5. Click **Get Started**, then **Next**.



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

6. Enter the **TRAQS URL** (<https://mpp.nasdaq.com> (production) **OR** <https://mpp-test.nasdaq.com> (NTF) in the **New Account** text box , then click **Next**.
Note: If you encounter any errors during this step, please refer to the following [link](#).

The screenshot shows the Okta Verify interface. At the top left is the 'Okta Verify' logo and a 'Back' link. The main content is split into two columns. The left column is titled 'New account' and contains a text input field, a blue 'Next' button, and a link for 'Need help signing in?'. The right column is titled 'Add account from another device' and contains a paragraph of text: 'If you have an Okta Verify account on another device, you can add it to this device.' Below this text is a blue 'Add account' button.

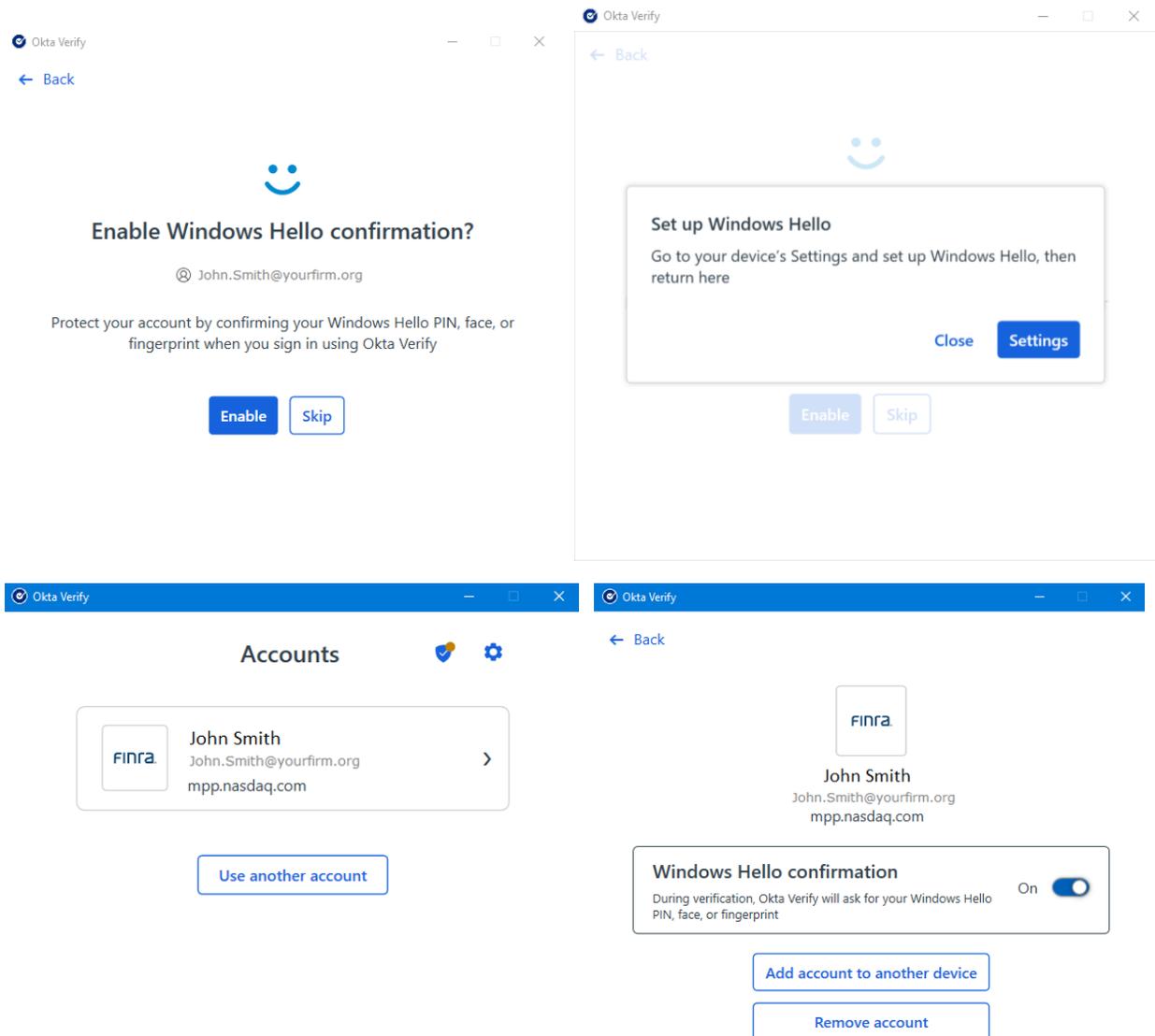
7. Enter your TRAQS **Username (email address)**, click **Next**. Enter **Password**, click **Verify**.
Note: If you are already enrolled with another MFA, the system may ask you to verify with your Username (email address), Password and Authentication Method.

The first screenshot shows the FINRA 'Sign In' page. It features the FINRA logo at the top, followed by the text 'Sign In'. Below this is a text input field labeled 'Username (email address)', a blue 'Next' button, and three links: 'Unlock account?', 'Forgot password?', and 'Help'.

The second screenshot shows the 'Verify with your password' page. It features the FINRA logo at the top, followed by a circular icon containing a lock and the text '****'. Below this is the text 'Verify with your password' and the email address '@ John.Smith@yourfirm.org'. There is a text input field labeled 'Password' with a toggle icon, a blue 'Verify' button, and two links: 'Forgot password?' and 'Back to sign in'.

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

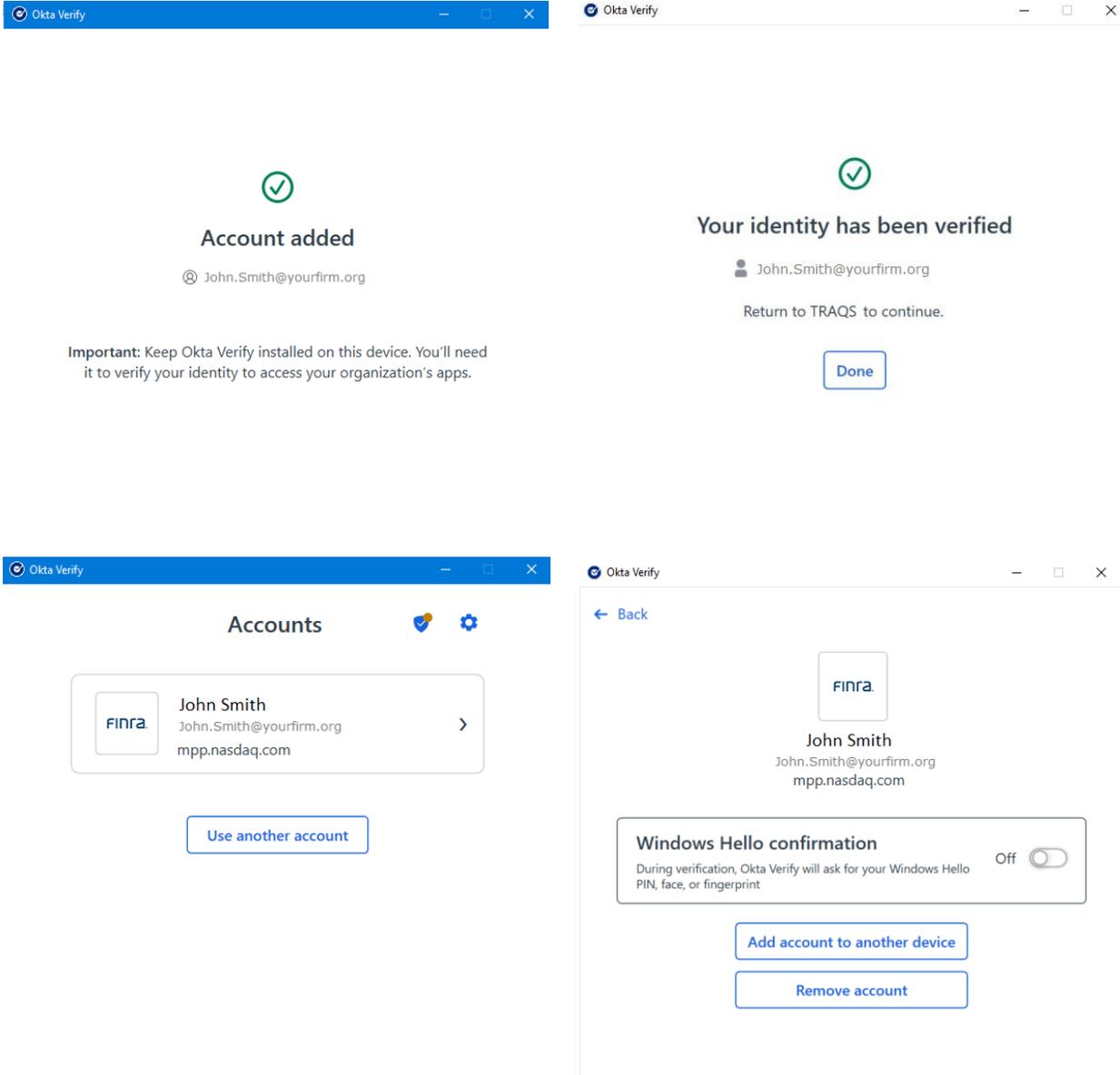
- The user can enable Windows Hello confirmation to be used with Okta Verify FastPass (Desktop). Click on the **Enable** button and follow the prompts to set up Windows Hello. **Note:** This may be controlled by your firm's desktop support team. If you are able to set yourself up with no policy restrictions and your machine supports it, the user refer to the OS support documentation found [here](#).



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

9. If you choose not to configure Windows Hello confirmation click **Skip** to continue.
Your account will be added, click **Done** on verified screen.

Note: If you choose not to configure Windows Hello confirmation you can set it up at a later time.



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

10. Once you have completed the verification set up, you will be directed back to the **Set up security methods** screen with rest of available verification choices. Please continue reading for a description of each authentication method and instructions for enrollment.
11. Select **Continue** if you are finished setting up your authentication methods. Please see [How to Remove My Security Methods](#) below for information about removing Security Methods
12. 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.
13. The website will prompt you to use your chosen security method(s) to login.

Note: Okta Verify FastPass has **push notification or Windows Hello confirmation**.

| | |
|---|--|
| Push: Access the Okta Verify application on the associated desktop and approve the request with a click | Windows Hello Confirmation: Access the Okta Verify app on the associated device and approve the request. |
|---|--|

The screenshot shows the Okta Verify interface. At the top, the Okta Verify logo is visible. Below it, the FINra logo is displayed. The main heading is "Verify it's you with a security method" for the user John.Smith@yourfirm.org. There are two options: "Use Okta FastPass Okta Verify" with a "Select" button, and "Back to sign in". To the right, there is a "Are you trying to sign in?" section with a list of accounts: John.Smith@yourfirm.org, Okta Dashboard, and mpp.nasdaq.com, with "Yes, it's me" and "No, it's not me" buttons.

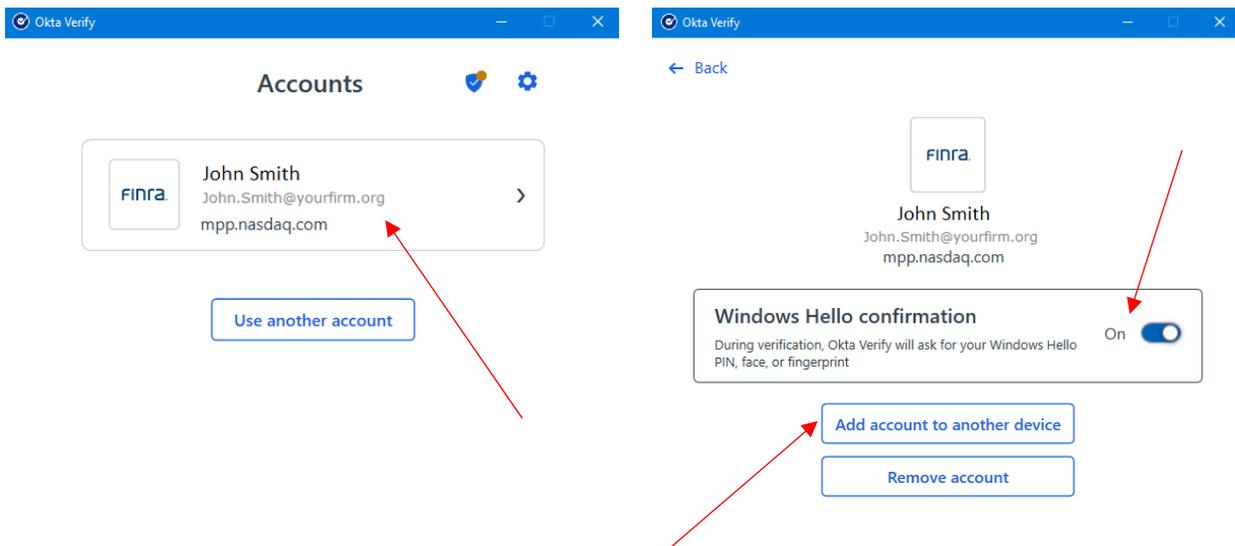
Below the main interface, two Windows Security dialog boxes are shown. The first dialog, titled "Making sure it's you", asks to confirm login to https://mpp-test.nasdaq.com/ through Okta Verify and displays "Hello, Smith, John! Select OK to continue." with "More choices", "OK", and "Cancel" buttons. The second dialog, also titled "Making sure it's you", asks to confirm login to the same URL and shows a PIN input field with a "PIN" label, an "I forgot my PIN" link, and "OK" and "Cancel" buttons.

Adding an Account from Another Device

If you already have an existing Okta Verify account and want to authenticate with the same account on another device, you can sync your devices using Bluetooth. By doing so, you can add your existing Okta Verify account directly to the other device without signing in to the End-User Dashboard.

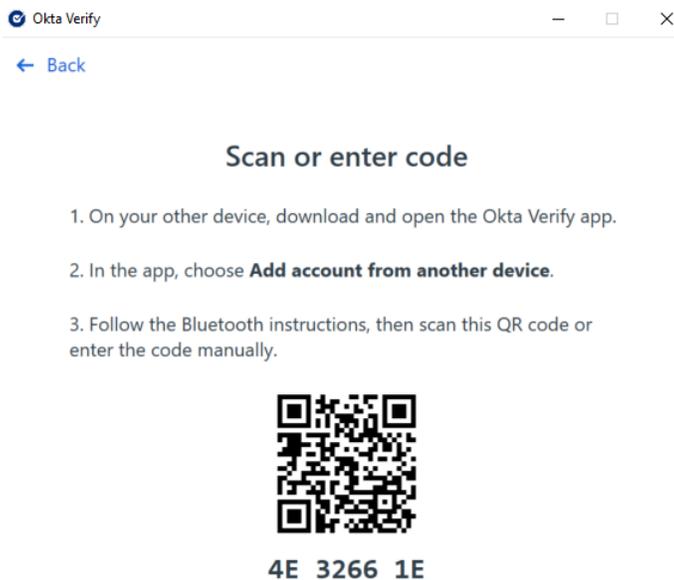
Note: You must have biometrics enabled on your “source” device. Check the settings app to confirm.

1. Start on the “source” Windows device where you already have an Okta Verify (Desktop) account. **Open the application**, click on **the account that you want to add to the “destination” device**. Click **Add account from another device** and **confirm your login to TRAQS through Windows Hello**. **Note:** Windows Hello confirmation has to be enabled on the “source” device.

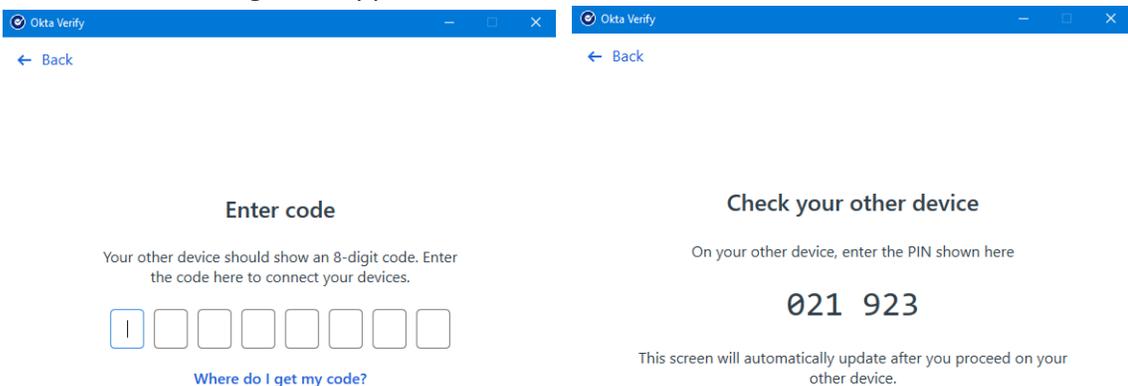


Enrolling in Multi Factor Authentication (MFA) to Access TRAQs Website and API

2. A **QR code and a code with numbers and letters** appear. Keep them handy. You will be prompted for the code in a later step.

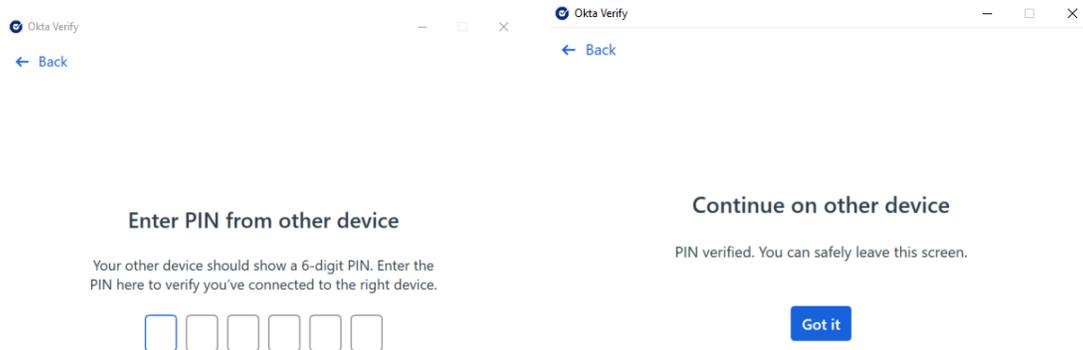


3. **Install Okta Verify (Desktop)** on the "destination" Windows device.
Note: This example is adding Desktop to Desktop, but you can add a mobile device this as well.
4. **Open the application**, click on **Add account from another device**. For this step, you will need the code generated by Okta Verify in the second step. **Enter the 8-digit code that is displayed on the "source" device into the "destination" device**. If the account setup is successful, a 6-digit PIN appears.



Enrolling in Multi Factor Authentication (MFA) to Access TRAQ5 Website and API

5. Confirm that you're pairing the right devices. **Enter the 6-digit PIN displayed in Okta Verify on the “destination” device into the “source” device.** If the PIN is correct, you receive a confirmation message.

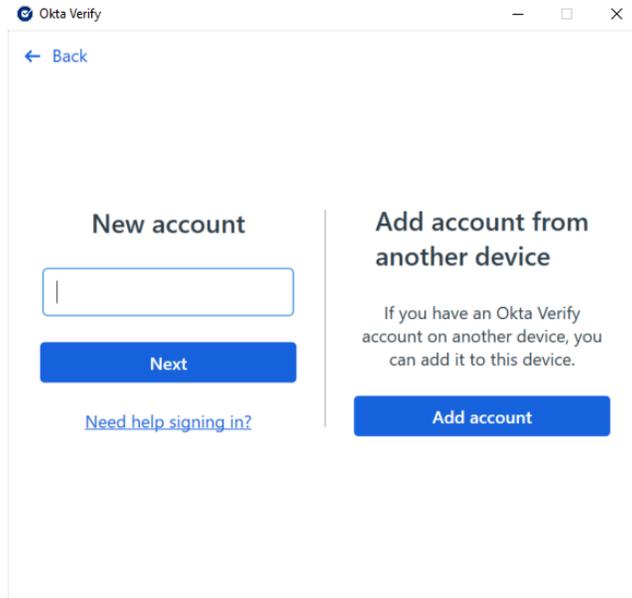


6. On the **“destination” device**, follow the Okta Verify instructions to complete the account setup.
7. You can now authenticate with Okta Verify on the **“destination” Windows device.**

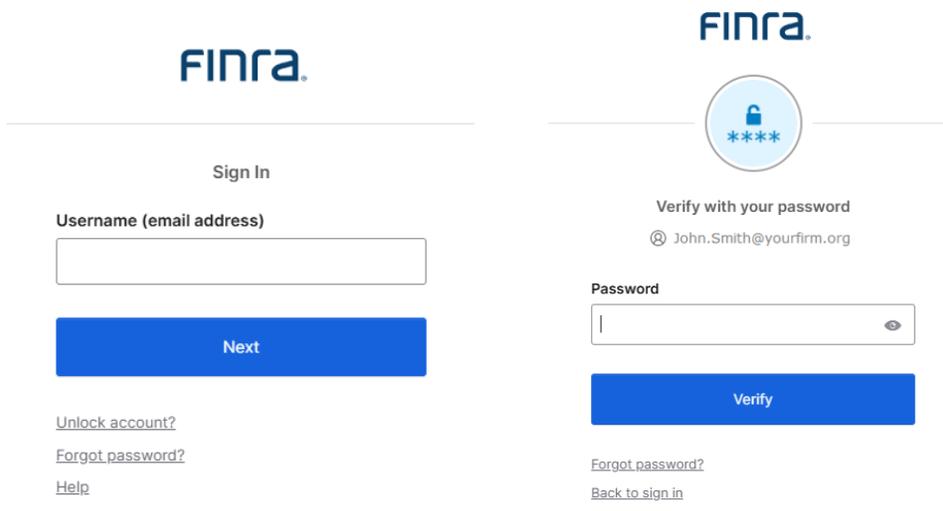
Use Another Account

1. Enter the **TRAQS URL** (<https://mpp.nasdaq.com> (production) **OR** <https://mpp-test.nasdaq.com> (NTF)) in the **New Account** text box , then click **Next**.

Note: If you encounter any errors during this step, please refer to the following [link](#)



2. Enter your TRAQS **Username (email address)**, click **Next**. Enter **Password**, click **Verify**.
Note: If you are already enrolled with another MFA, the system may ask you to verify with your Username (email address), Password and Authentication Method.



3. Follow the Okta Verify instructions to complete the account setup.

Federated Single Sign-On (SSO)

Federated Identity Management (FIM), also known as Federated SSO, refers to the establishment of a trusted relationship between separate organizations and third parties, such as application vendors or partners, allowing them to share identities and authenticate users across domains.

Note: Federated SSO can take up to a week to set up.

Note: Users logging in through Federated SSO no longer require an additional MFA step, as the customer's identity provider (IDP) performs secure authentication.

Setting up Federated SSO

To connect with Federated SSO, the Federation between mpp.nasdaq.com (production) or mpp-test.nasdaq.com (NTF) and the firm's Identity Provider (IDP) needs to be setup. This is done between Nasdaq and the firm's Identity and Access Management team, which administers it.

Contact NASDAQ tech support at 212-231-5180 option 4 for assistance with setting up Federated SSO.

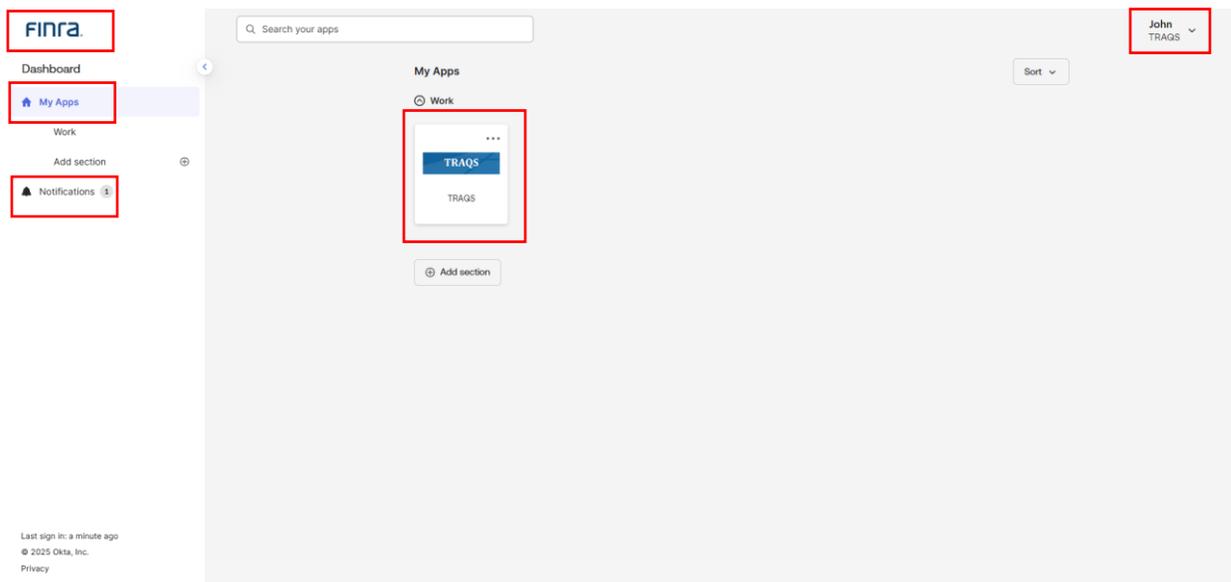
The questionnaire for setup:

1. To setup federation with a remote IDP for Federated Single Sign-On ("FedSSO") an exchange of SAML metadata as well as specific attribute sent by the customer's IDP are required. Nasdaq can provide the SP metadata of Nasdaq Sign In in advance if required.
2. Firms are required to send the authenticating user's email address as a SAML attribute, ideally called "email". The Subject NameID must be present, but is not evaluated. Transient NameID is acceptable, but email address is preferred.
3. Both IDP and SP initiated login is supported by Nasdaq, as well as optionally encrypted SAML assertions. RelayState for IDP initiated logins can be provided after federation is complete.
4. SAML Responses by the firm must be signed, AuthnRequests by Nasdaq can optionally be signed as well.

Please see [Section 3](#) below for instructions on logging into the TRAQ5 website using Federated SSO.

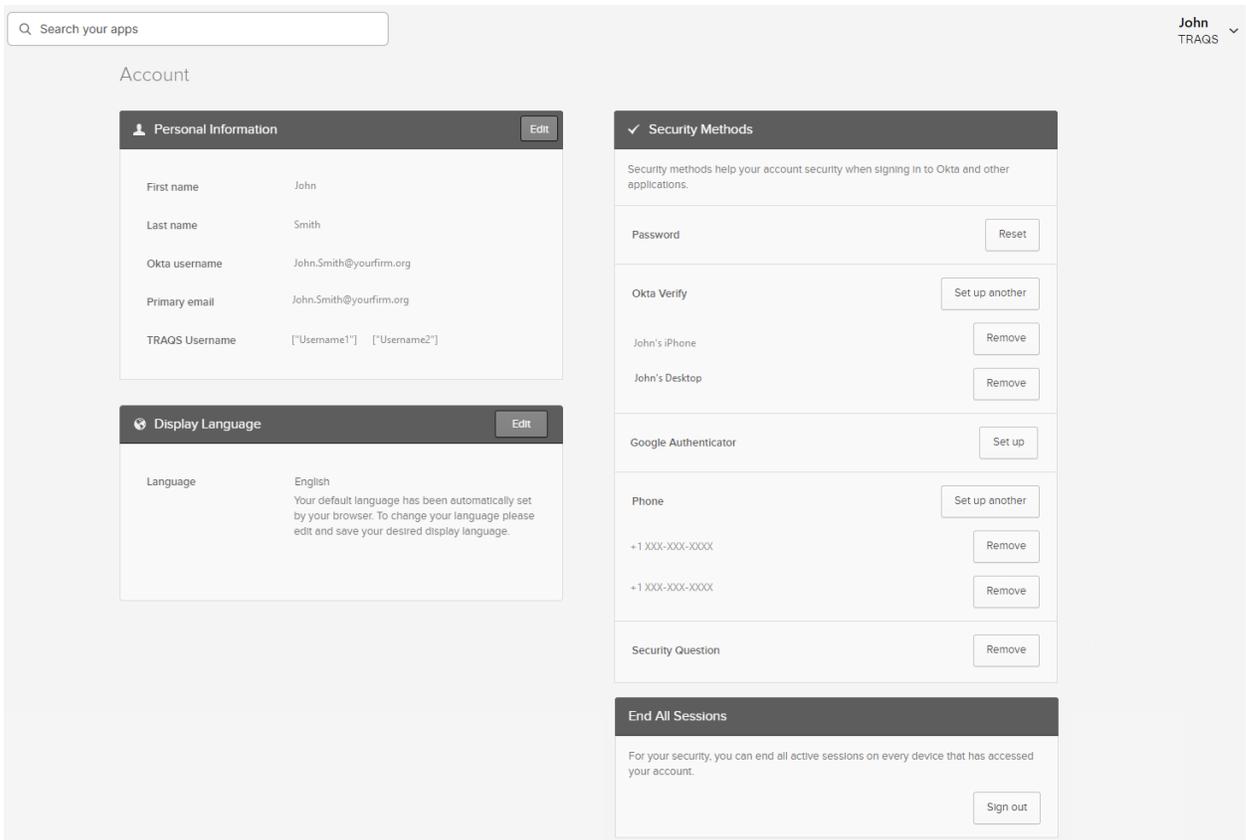
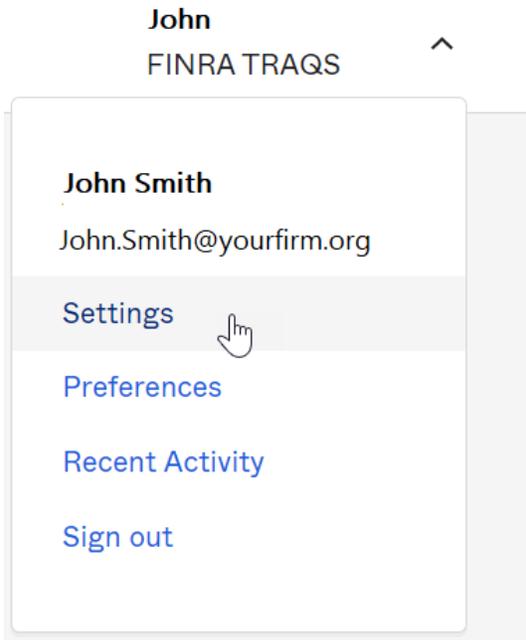
Section 2: Profile Page (Okta Dashboard)

1. Visit the NTF (UAT)website <https://mpp-test.nasdaq.com> OR Production website <https://mpp.nasdaq.com>
2. Enter your **Username (email address)**, click **Next**.
Note: Users logging in with Federated SSO will enter just their username
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. The Main Page (Home page) is where the link to the TRAQS Application resides
7. The Vertical Menu. This is where you can find:
 - FINRA Logo** – Click to return to the Main Page (Home page)
 - My Apps** – Where the link to the TRAQS Application resides
 - Notifications** – Click to view any notifications
8. The Horizontal Menu. This is where you can find:
 - User Profile (Your Name):**
 - **My Settings** - Select to go to the Account Page
 - **Preferences** – Select to change the Layout or Pop up messages timer
 - **Recent Activity** – Select to view the Sign-ins and Security Events information
 - **Sign out** – Select to Sign out of the Profile Page



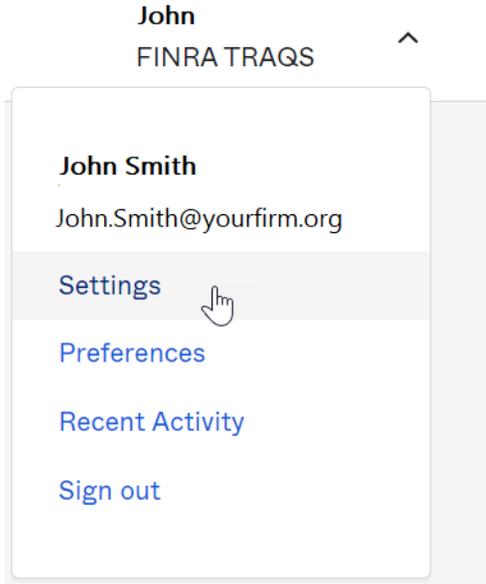
Enrolling in Multi Factor Authentication (MFA) to Access TRAQs Website and API

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



How to Edit the User Profile

1. Visit the NTF (UAT) website <https://mpp-test.nasdaq.com> OR Production website <https://mpp.nasdaq.com>.
2. Enter your **Username (email address)**, click **Next**.
Note: Users logging in with Federated SSO will enter just their username
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.



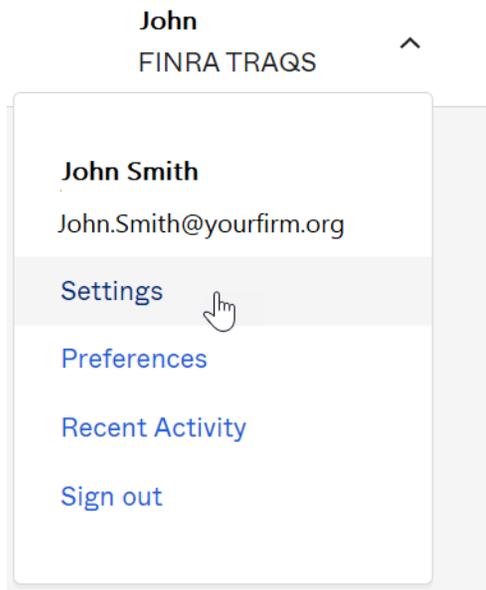
7. Users are able to update the information in the profile screen by clicking the **Edit** button beside the profile item. **Note:** Security Methods will not have the edit button.
8. Users can not edit the personal information section of this site. If your primary email or phone number need updating, please contact **FINRA Market Operations at 1-866-776-0800 option 2** or FINRAOperations@finra.org.
9. 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.”

10. To **Remove a Security Methods(s)**: See the next section in this document [How to Remove My Security Method\(s\)](#) for instructions.
11. To **Set up a Security Methods(s)**: See the next section in this document [How to Add a Security Method\(s\)](#) for instructions.
12. To **Remove your Security Question**: Click the **Remove** in the Security Question section 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 prompts.
13. To **Change the Display Language** of the profile screen: click on that **Edit** button and select the language you prefer from the drop down, click **Save**.
14. To **End All Sessions**: Click **Sign out** in the End all sessions section, a popup asking “You’ll be signed out of all active sessions using your account on every device, including your browser.” will come up, click Sign out. This is a security feature which can end all active sessions on every device that has accessed your account
NOTE: Clicking on the **Sign out** button under the **End All Sessions** section of the Okta Dashboard **will Inactivate/Revoke ALL Refresh Tokens**.

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

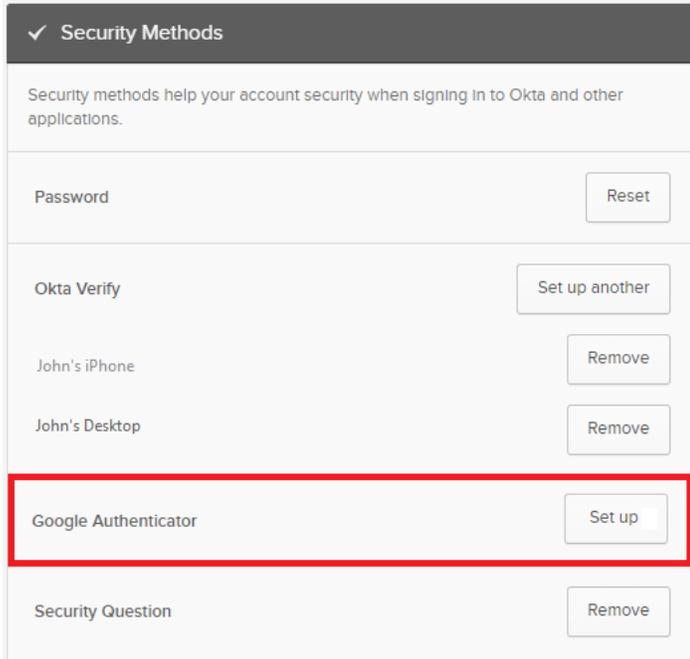
How to Add a Security Method(s)

1. Visit the NTF (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.



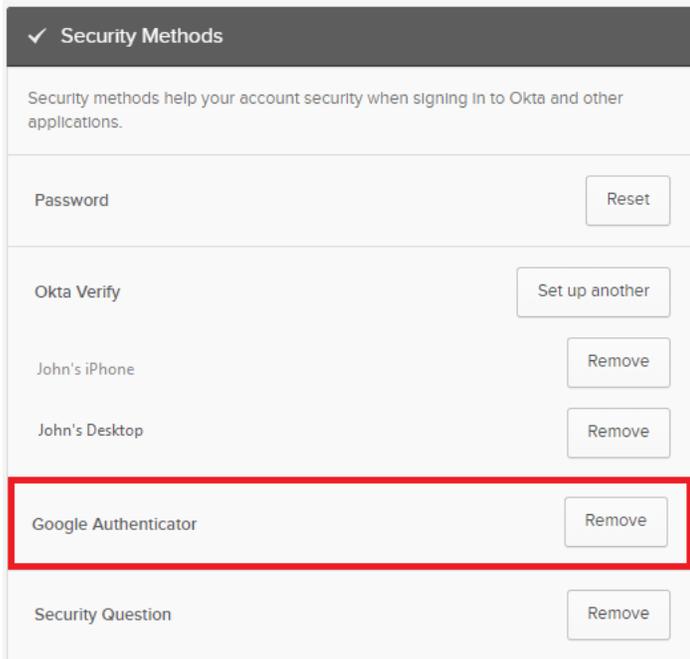
Enrolling in Multi Factor Authentication (MFA) to Access TRAQs Website and API

- Under the Security Methods click **Setup or Setup Another** beside the authentication method you want to setup and follow the prompts OR review the appropriate set up instructions in Section 1 of this document. **Note:** In the following example we are adding Google Authenticator.



The screenshot shows the 'Security Methods' interface. At the top, there is a header with a checkmark and the text 'Security Methods'. Below this is a sub-header 'Security methods help your account security when signing in to Okta and other applications.' The main content area lists several authentication methods, each with a corresponding button: 'Password' with a 'Reset' button; 'Okta Verify' with a 'Set up another' button; 'John's iPhone' with a 'Remove' button; 'John's Desktop' with a 'Remove' button; 'Google Authenticator' with a 'Set up' button; and 'Security Question' with a 'Remove' button. A red rectangular box highlights the 'Google Authenticator' row, specifically the 'Set up' button.

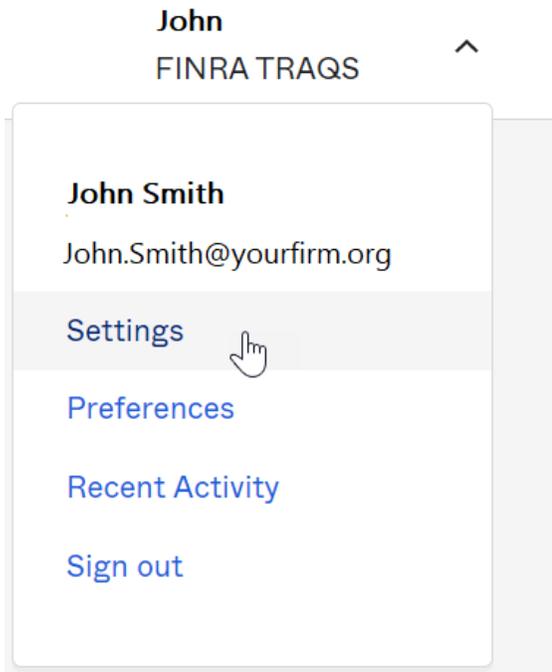
- When completed you will be directed back to the profile page and the button beside the authentication method will now say **"Remove"**. **Note:** If you were adding Okta Verify the button would say **"Set up another"**.



This screenshot shows the same 'Security Methods' interface as the previous one, but the 'Google Authenticator' row is now highlighted with a red rectangular box, and the button next to it has changed from 'Set up' to 'Remove'. All other elements, including the header, sub-header, and other authentication methods, remain the same.

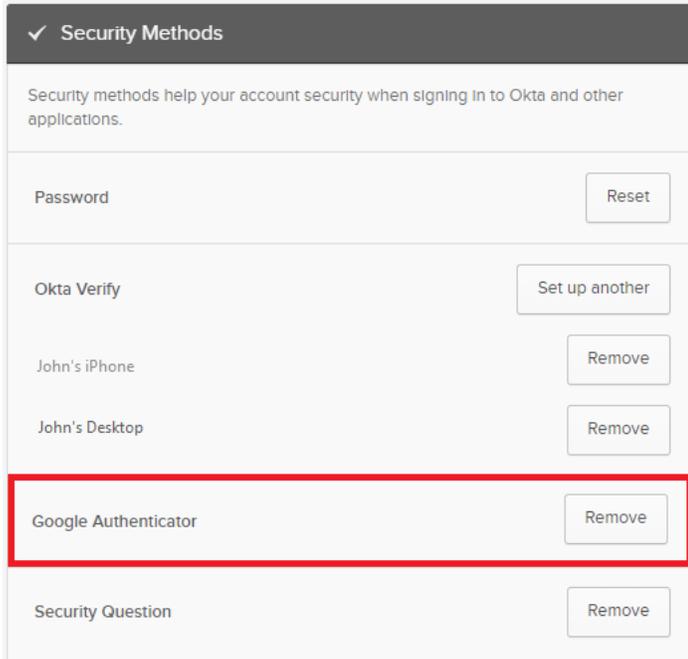
How to Remove a Security Method(s)

1. Visit the NTF (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.



Enrolling in Multi Factor Authentication (MFA) to Access TRAQ5 Website and API

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

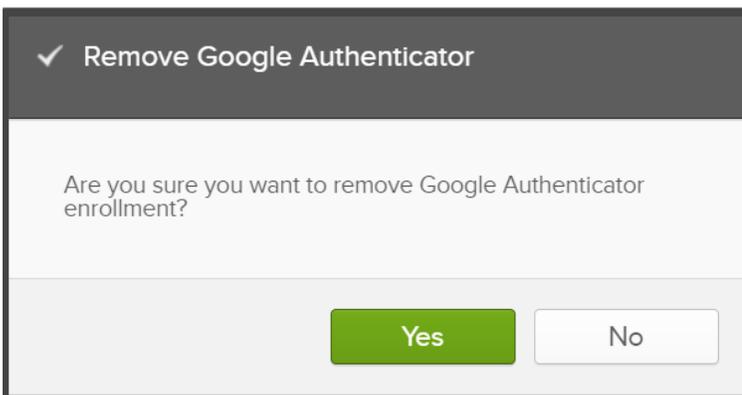


✓ Security Methods

Security methods help your account security when signing in to Okta and other applications.

| | |
|----------------------|----------------|
| Password | Reset |
| Okta Verify | Set up another |
| John's iPhone | Remove |
| John's Desktop | Remove |
| Google Authenticator | Remove |
| Security Question | Remove |

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



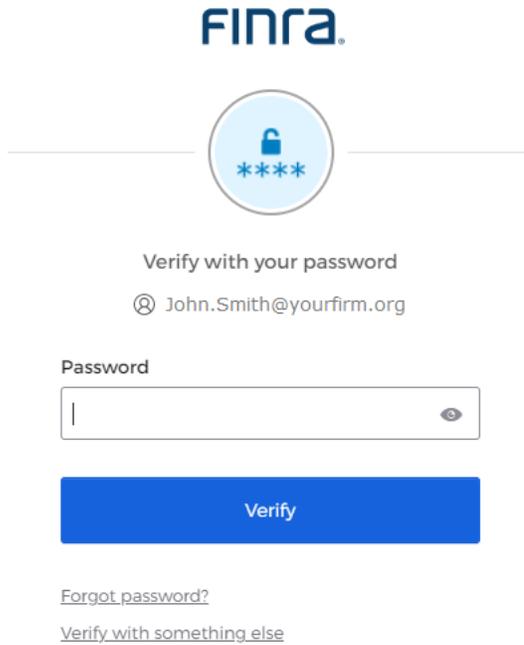
✓ Remove Google Authenticator

Are you sure you want to remove Google Authenticator enrollment?

Yes No

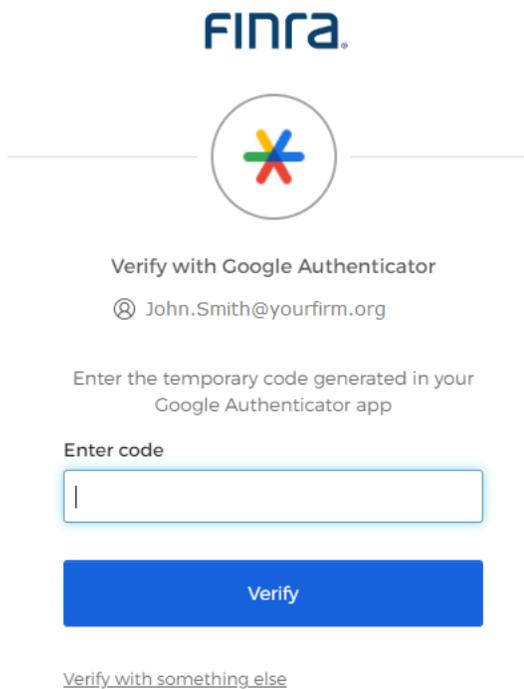
Enrolling in Multi Factor Authentication (MFA) to Access TRAQ5 Website and API

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



The screenshot shows the FINRA login interface for password verification. At the top is the FINRA logo. Below it is a circular icon containing a padlock and four asterisks. The text reads "Verify with your password" followed by the email address "John.Smith@yourfirm.org". There is a "Password" label above a text input field with a visibility toggle icon. A blue "Verify" button is positioned below the input field. At the bottom, there are two links: "Forgot password?" and "Verify with something else".

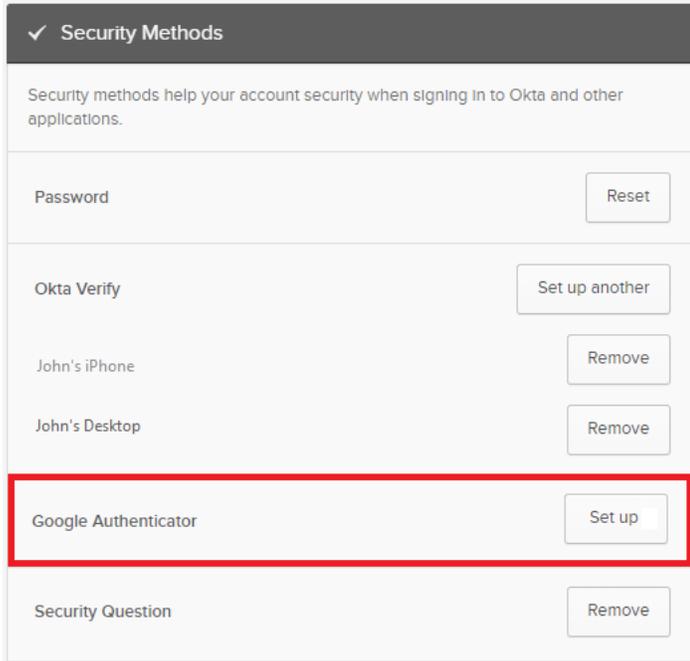
10. Verify with Factor.



The screenshot shows the FINRA login interface for Google Authenticator verification. At the top is the FINRA logo. Below it is a circular icon containing the Google Authenticator logo. The text reads "Verify with Google Authenticator" followed by the email address "John.Smith@yourfirm.org". Below this, it says "Enter the temporary code generated in your Google Authenticator app". There is an "Enter code" label above a text input field. A blue "Verify" button is positioned below the input field. At the bottom, there is a link: "Verify with something else".

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

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.”



| ✓ Security Methods | |
|---|----------------|
| Security methods help your account security when signing in to Okta and other applications. | |
| Password | Reset |
| Okta Verify | Set up another |
| John's iPhone | Remove |
| John's Desktop | Remove |
| Google Authenticator | Set up |
| Security Question | Remove |

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

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



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](#) [\[mpp.nasdaq.com\]](http://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.

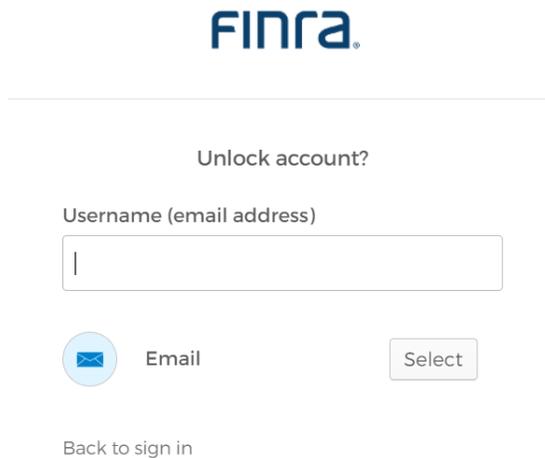
Note: You must have at least one security method set up in order to access the TRAQS website.

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**.



FINRA

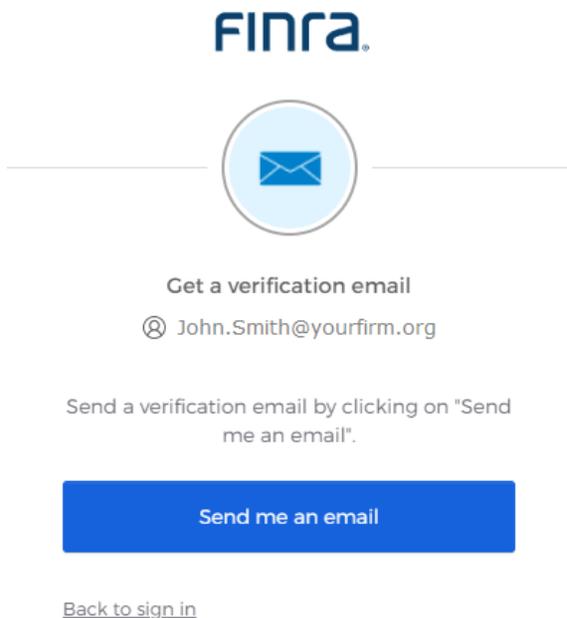
Unlock account?

Username (email address)

Email

[Back to sign in](#)

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



FINRA



Get a verification email

 John.Smith@yourfirm.org

Send a verification email by clicking on "Send me an email".

[Back to sign in](#)

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

FINRA[®]



Verify with your email

👤 John.Smith@yourfirm.org

⚠️ Haven't received an email? [Send again](#)

We sent you a verification email. Click the verification link in your email to continue or enter the code below.

[Enter a verification code instead](#)

[Back to sign in](#)

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



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

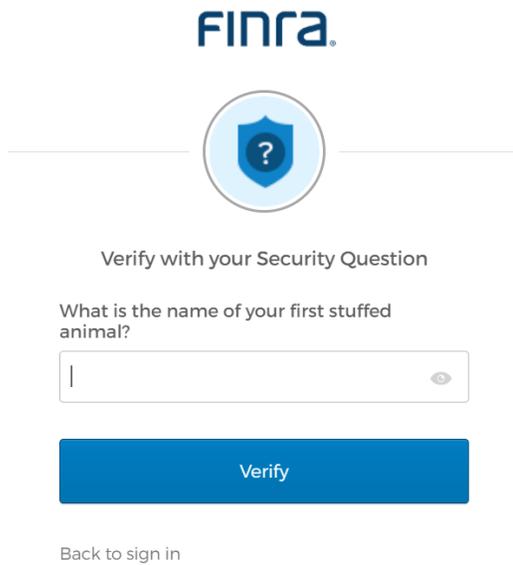


Alternatively you can enter this code: 540149

This link expires in 5 minutes.

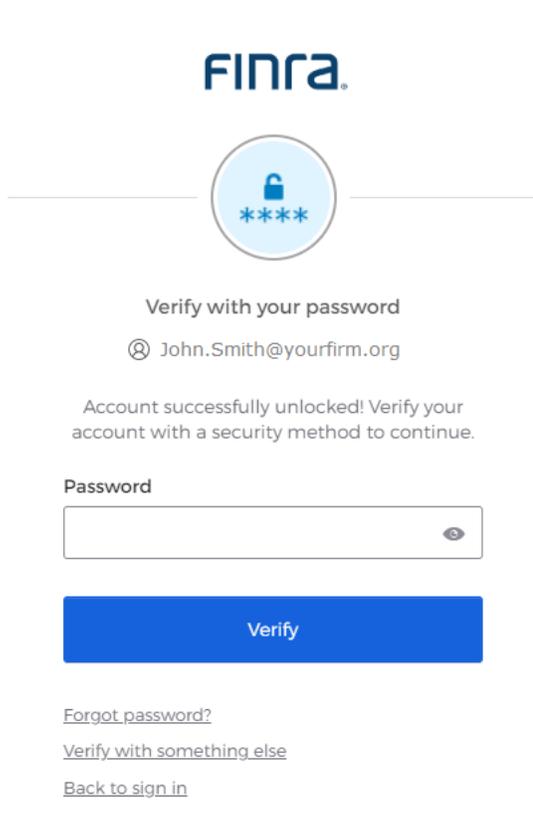
For further information regarding MFA for TRAQS please click [here](#)

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



The screenshot shows the FINRA logo at the top. Below it is a circular icon containing a shield with a question mark. The text reads "Verify with your Security Question". The question is "What is the name of your first stuffed animal?". There is a text input field with a cursor and a small eye icon to its right. Below the input field is a blue "Verify" button. At the bottom, there is a link that says "Back to sign in".

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



The screenshot shows the FINRA logo at the top. Below it is a circular icon containing a padlock and four asterisks. The text reads "Verify with your password". Below this is the email address "John.Smith@yourfirm.org" with a small icon to its left. A message states "Account successfully unlocked! Verify your account with a security method to continue." Below the message is the label "Password" and a text input field with a cursor and a small eye icon to its right. Below the input field is a blue "Verify" button. At the bottom, there are three links: "Forgot password?", "Verify with something else", and "Back to sign in".

Enrolling in Multi Factor Authentication (MFA) to Access TRAQ5 Website and API

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



Verify it's you with a security method

 John.Smith@yourfirm.org

Select from the following options

-  Google Authenticator
-  Enter a code
Okta Verify
-  Get a push notification
Okta Verify
-  Use Okta FastPass
Okta Verify

[Back to sign in](#)

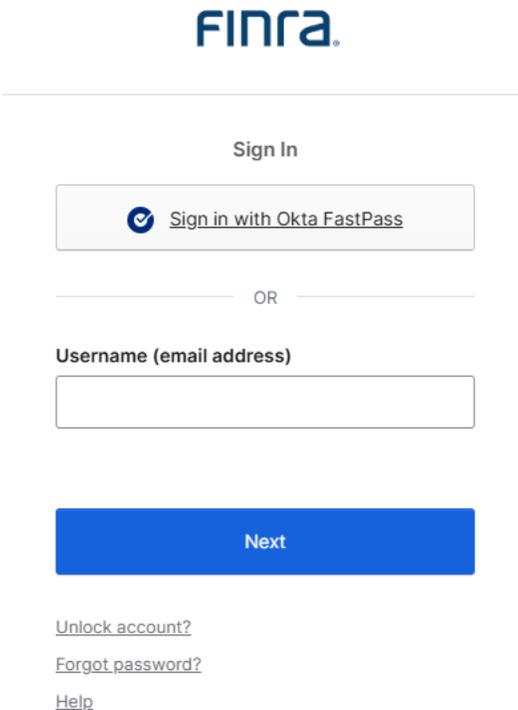
Note: Your account automatically unlocks after 15 minutes. If you do not act on the unlock email within 15 minutes your account will automatically unlock.

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**.
Note: Users logging in thorough Federated SSO will automatically be logged into TRAQS website.

A screenshot of the FINRA Sign In page. At the top center is the FINRA logo. Below it is the text 'Sign In'. There is a button with a checkmark icon and the text 'Sign in with Okta FastPass'. Below this button is the word 'OR' centered between two horizontal lines. Underneath is the label 'Username (email address)' followed by an empty text input field. At the bottom of the form is a large blue button with the text 'Next'. Below the 'Next' button are three links: 'Unlock account?', 'Forgot password?', and 'Help'.

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




Verify with your password

 John.Smith@yourfirm.org

Password

[Verify](#)

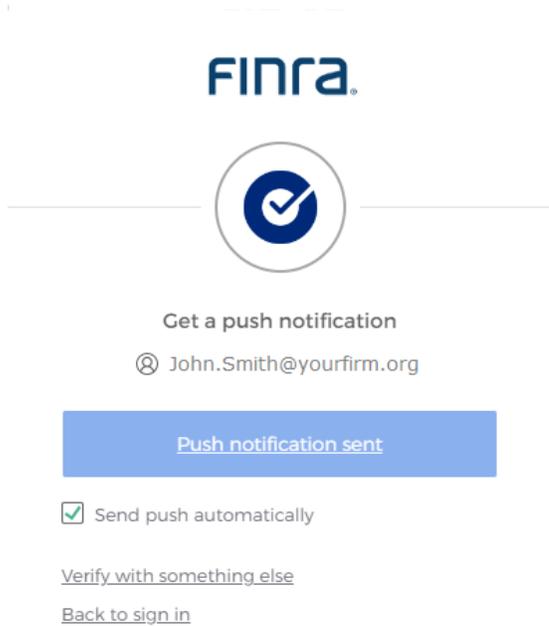
[Forgot password?](#)

[Verify with something else](#)

[Back to sign in](#)

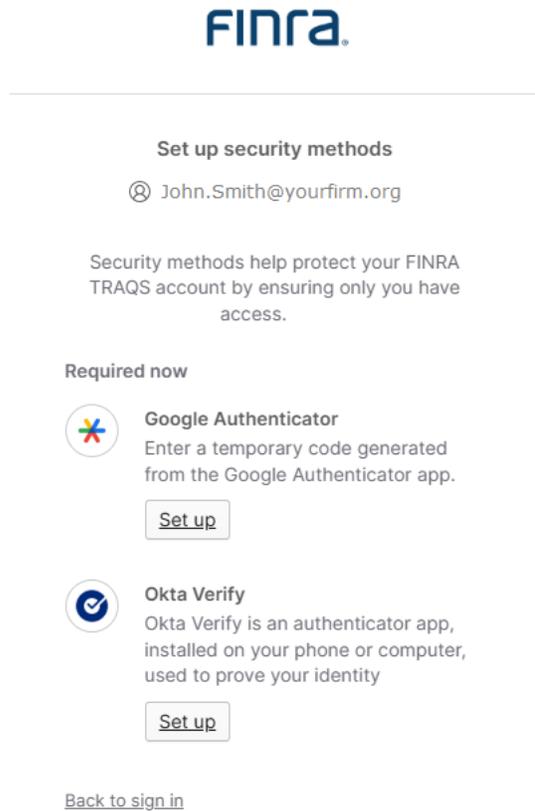
Enrolling in Multi Factor Authentication (MFA) to Access TRAQS Website and API

4. The system defaults to the last used security method to log you in. (In the following example we are using Okta Verify Mobile (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.



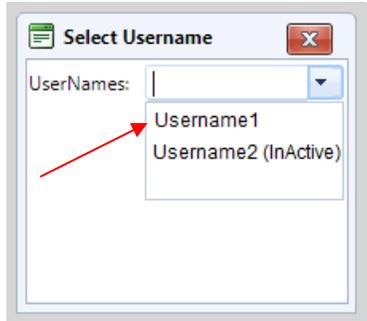
Enrolling in Multi Factor Authentication (MFA) to Access TRAQS Website and API

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.



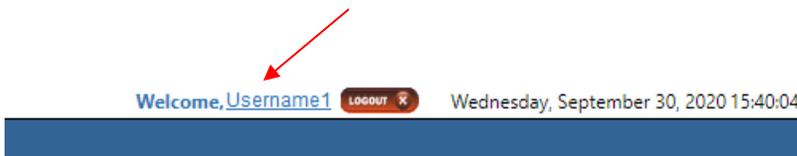
5. **If a user has only one username associated with their Username (email address), users will be directed into the TRAQS website.**

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

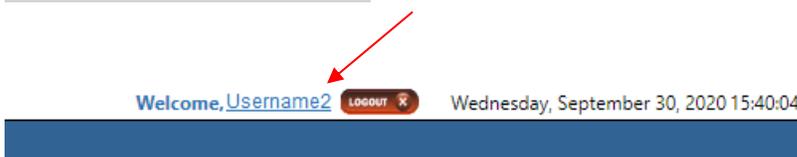
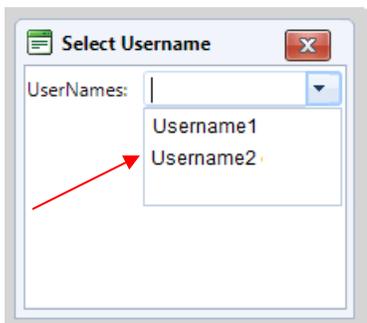


Note: If your username in the drop down above has “InActive” beside it. Please contact your Super Account Administrator and have them reset your account to active in PDM.

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.

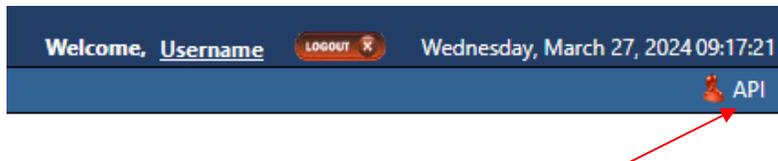


Section 4: How to Access the API Download (Manual)

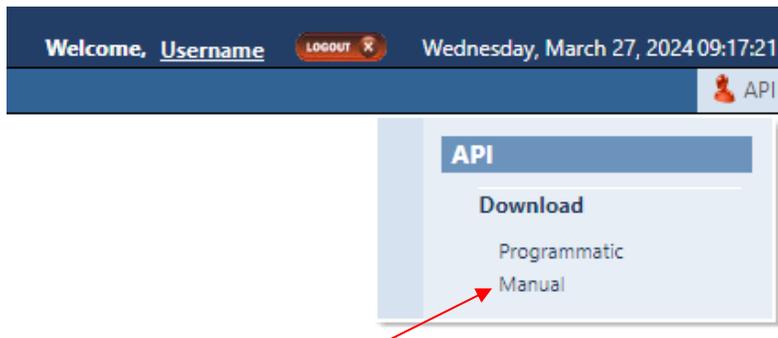
Users with API access are required to complete the steps outlined in [Section 1](#) of this document prior to downloading the API files via web. Please see the individual FINRA product API Specification document for the specific facility to learn more about the individual files.

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.

➤ [API / Download / Manual](#)

Action: Facility: File: Day:

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:

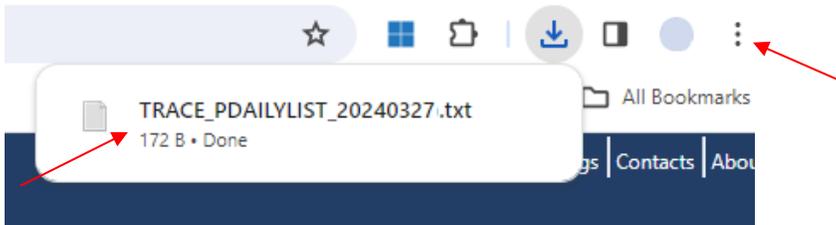
Note: Day is used for Daily List requests with Action of "Download" only. Day will not be available for Daily List requests with an Action of "Delta."

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

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

- **DOWNLOAD REQUEST SENT...**
- **DOWNLOAD COMPLETE.**

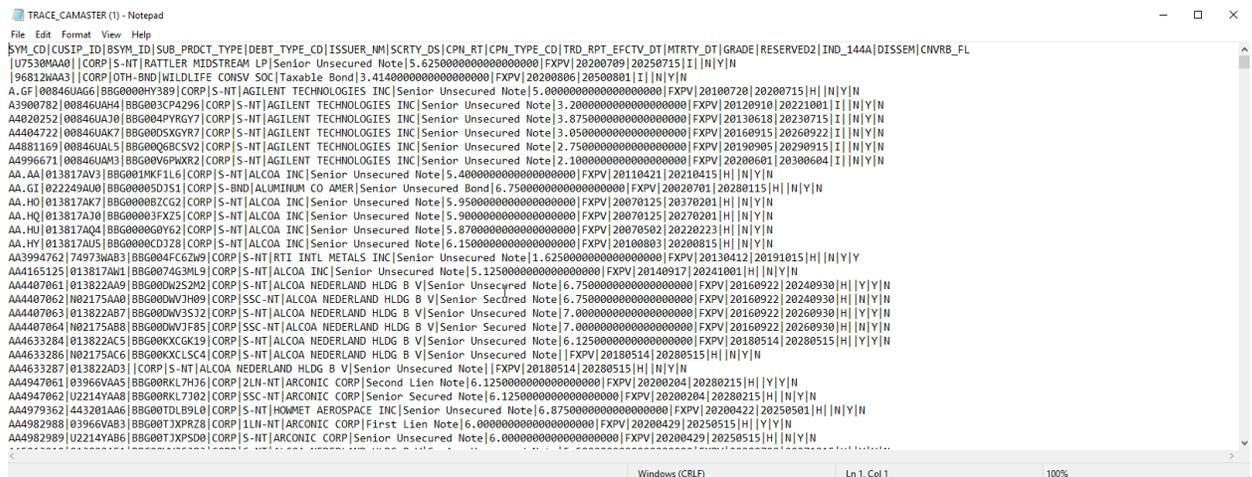
6. Click on the **popup** to open the downloaded file.



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.

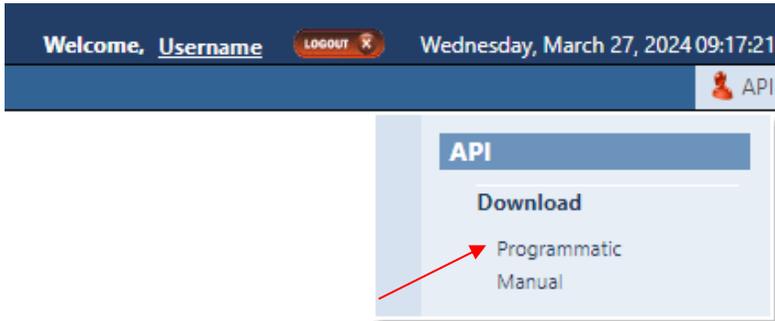
To access TRAQS, a username, password, and NASDAQ Multi-Factor Authentication (MFA) is required. To establish a TRAQS username, please consult your Super Account Administrator (SAA) and use the Participant Data Management (PDM) system.

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**.

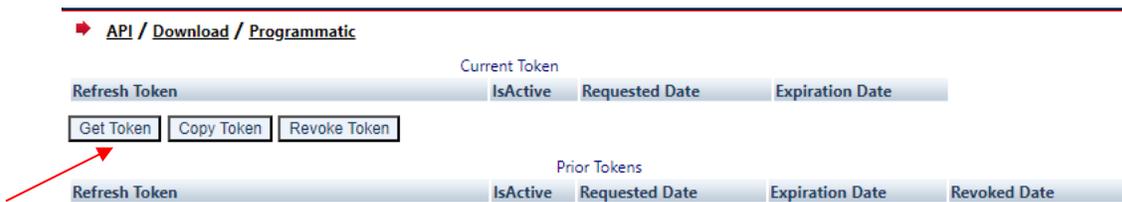


Enrolling in Multi Factor Authentication (MFA) to Access TRAQS Website and API

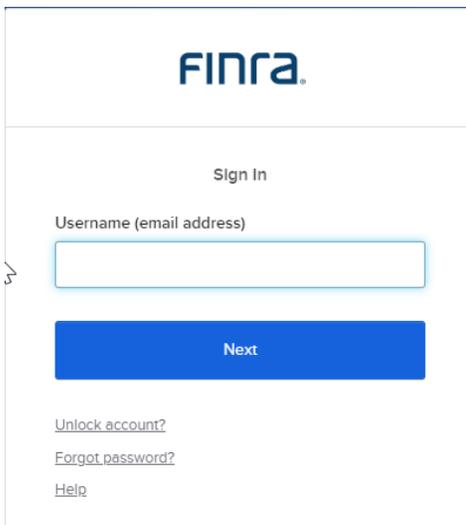
4. Click **Programmatic** from the **Download Menu** (this is where the Refresh Token is obtained).



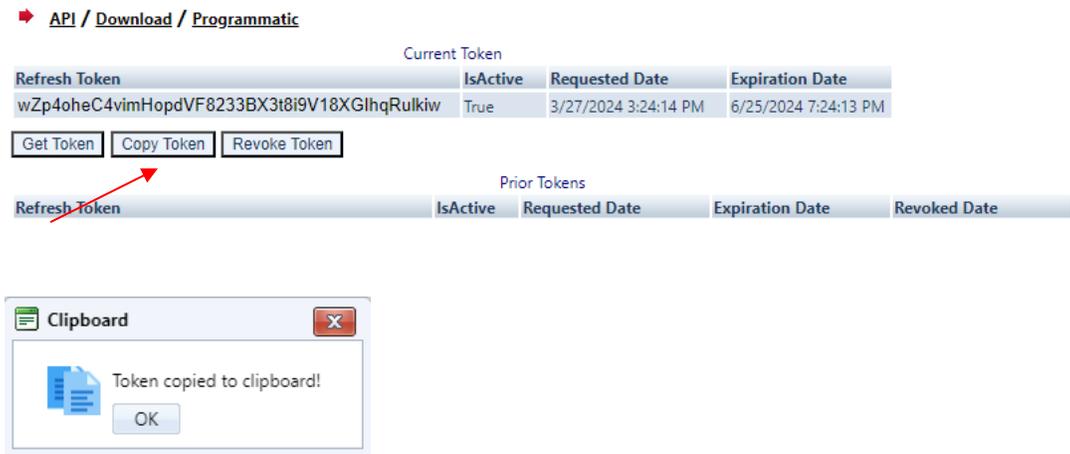
5. Click **Get Token** from the **API Download Programmatic** screen.



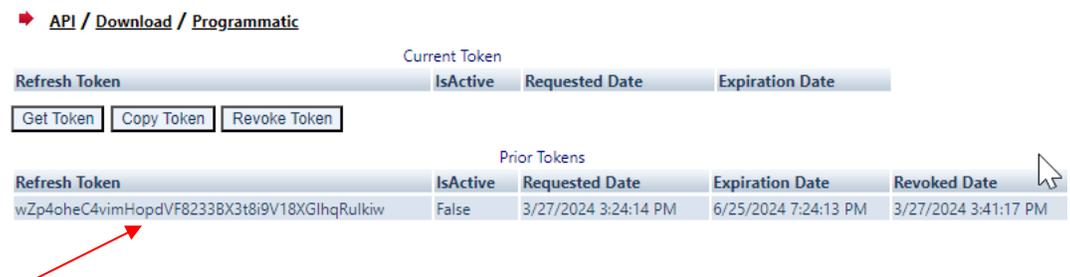
6. After requesting the Refresh Token the system will ask you to **Authenticate** again. If successful the user will be brought back to the API Download Programmatic screen and the Refresh Token information will be populated under the "Current Token" portion of the screen.



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



- Add code to your script to request an **Access Token**.
- Upon logging into the API domain from your application, your application will request a new Access Token from the TRAQS download server.
- Your application will apply the new Access Token to the download API request call.
- On success, the requested data will be returned to your application.
- 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.



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

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.

➤ [API / Download / Programmatic](#)

Current Token

| Refresh Token | IsActive | Requested Date | Expiration Date |
|--|----------|----------------------|----------------------|
| r7W5gnX_FLzliq-HPAm06dcJvlBhXUWNzKFJH31Rts | True | 3/27/2024 3:51:26 PM | 6/25/2024 7:51:26 PM |

Prior Tokens

| Refresh Token | IsActive | Requested Date | Expiration Date | Revoked Date |
|---|----------|----------------------|----------------------|----------------------|
| wZp4oheC4vimHopdVF8233BX3t8i9V18XGihqRulkiw | False | 3/27/2024 3:24:14 PM | 6/25/2024 7:24:13 PM | 3/27/2024 3:41:17 PM |

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 if not using Federated SSO.

Can a user have MFA and Federated SSO?

No, user accounts can be set to either authenticate via Federated SSO or locally through Okta.

Want to enroll in Federated SSO?

Review the Federated Single Sign-On (SSO) section in this document and contact NASDAQ tech support at 212-231-5180 option 4.

Having issues with Federated SSO?

Please contact your firms Identity and Access Management team.

Having issues Downloading Okta Desktop Application?

Please contact your firms Desktop Support.

Unable to enroll in Okta Verify Desktop, getting “The sign-in URL is not secure”?

Please see the solution in the following [link](#):

Having issues setting up Windows Hello?

Please contact your firms Desktop Support. Windows support documentation can be found [here](#).

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 Profile (Dashboard) 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 [How to Edit the User Profile](#) in 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.

How can I add a new Security Method?

Please see [How to Add a Security Method\(s\)](#) in Section 2 for instructions.

How can I remove a Security Method?

Please see [How to Remove a Security Method\(s\)](#) in Section 2 for instructions.

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 environments. 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.

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.

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.

[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.

[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: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Section 4: How to Access API Download (Manual) • Section 5: How to Access API Download (Programmatic) • Section 6: Common Questions |
| 08/20/2024 | 2.1 | Updated document to include information relevant for production release. Updates are as follows: <ul style="list-style-type: none"> • Section 6: Common Questions |
| 07/01/2025 | 2.2 | Updated document to include changes in the sign-on process: <ul style="list-style-type: none"> • Retirement of SMS and Voice Call Authentication (Phone) Methods • Addition of Okta Verify Desktop (Windows Hello) |

Enrolling in Multi Factor Authentication (MFA) to Access TRAQ5 Website and API

| | | |
|------------|-----|--|
| | | Authentication Method for the TRAQ5 Website. <ul style="list-style-type: none">• Addition of Federated Single Sign-On (SSO) for the TRAQ5 Website. |
| 03/16/2026 | 2.3 | <ul style="list-style-type: none">• Remove all references to Phone (SMS/Voice) MFA |