

Nasdaq Sign-in Access for Data-Client Portal

Introduction

Multi-factor authentication (MFA) is a multi-step account login process that requires users to provide information in addition to a password. It is used to validate a user's identity for access and helps prevent unauthorized users from accessing accounts, even in the event of a stolen password.

For Data-Client Portal authentication, you will use a platform called "Nasdaq Sign In" which is using infrastructure provided by "Okta".

In this guide, there are instructions for:

Part 1: Initial Set-up

1. Enable Multi-factor authentication
 - a. Google Authenticator
 - i. Shared reporting mailbox
 - b. Okta Verify
2. Organizational Restrictions for External Applications?
3. Using the Authenticator Extension

Part 2: Accessing Data-Client Portal for Usage Reporting

Assistance: DataOps@Nasdaq.com

Part 1: Initial Set-up

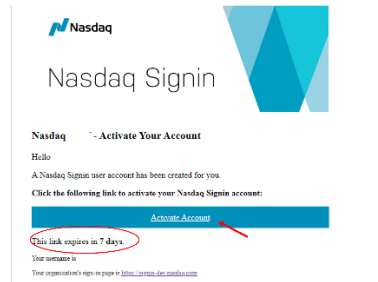
What you will need:

- "Welcome" email
- Mobile Device
- Verification App downloaded (See Page 3)

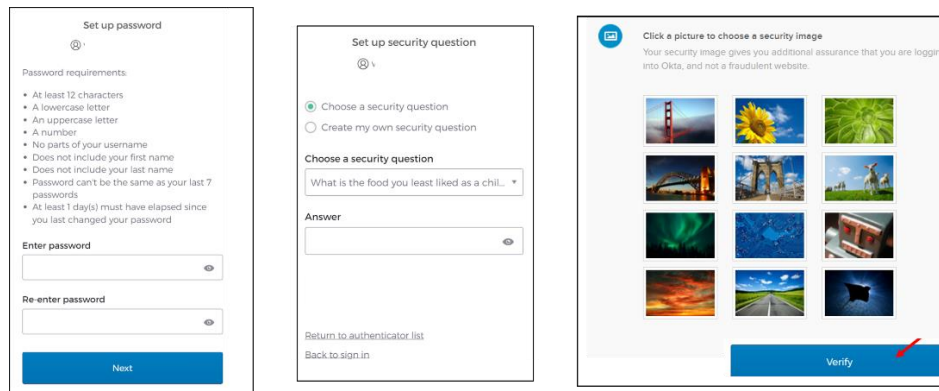
Step 1 When you are designated as a Reporter for Market Data usage, you will be emailed a "Welcome Message."

Open the "Welcome to Nasdaq Sign-in" message
Click on "Activate Account."

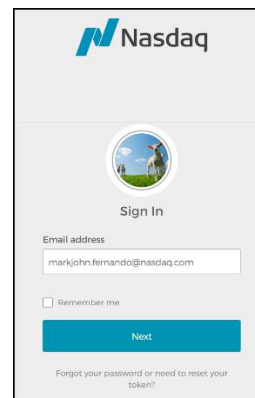
Please note: This link is only active for seven days (7) days. If it expires, contact DataOps@Nasdaq.com.



Step 2 Set Up Password, Security Question and Security Image. Once complete, click "Verify."



Step 3 You will be taken to the Sign-in Page. Enter your email address and click "Next."



- Step 4** You will be directed to the dashboard. Click on the “Data-Client Portal” Application Icon to begin enabling the Multi-factor Authentication process. (Note: This icon may say InfoMatch.)

Part 2: Enable Multi-factor Authentication

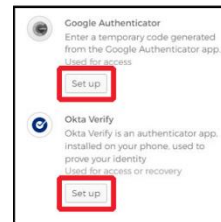
You will need to use an application to verify your account during set-up as well as every time you access the Data-Client Portal. You may use either Okta Verify or Google Authenticator.

Note:

- Okta Verify is recommended because it directly interfaces with the Okta platform
- Google Authenticator is recommended if you use a shared email for reporting (See page 4)
- If you cannot use a mobile device, there is a Google Extension that can be uploaded to your computer. Directions begin on Page 7.

- Step 1** Click “Set-up” for the application you select.

When you open the application, there are step-by-step set-up instructions.

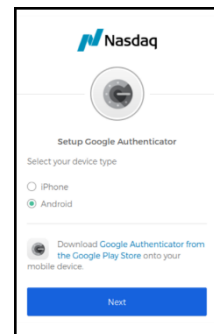


Using Google Authenticator

- Step 1** Select your mobile device. You will be redirected to the Apple App Store for iPhones or Google Play for Androids.

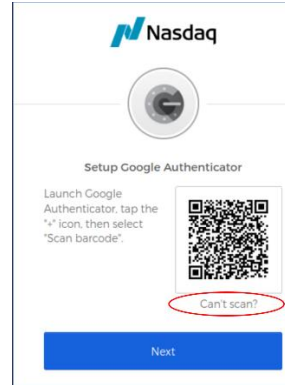
Click “Next” and download the App.

Note: Set-up is the same for either type of device.



Step 2 After installing the application, open it and click on the "+" icon in the lower right corner (design may vary).

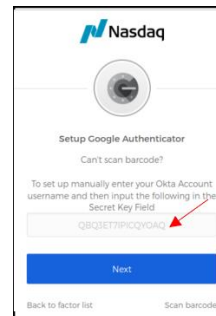
Tap "Scan barcode". Your camera will open and scan the QR code. A message will notify you when the scan was successful.



If you cannot scan the QR code, please click on "Can't scan?".

Copy the "Secret Key Field" and click Next.

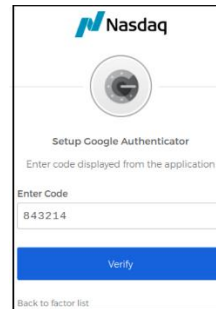
Enter your password and the "Secret Key Field" and click Next.



Step 3

Verify your setup by inputting the current code displayed in "Authenticator Codes" on the App.

Click "Verify."



Shared Reporting Mailbox

If you use one general email address for reporting by multiple usage reporters (For example: DataReporting@123Bank) use Google Authenticator as your Autenticaion App.

Here's what you'll do:

1. One person should click on the "Welcome" email and follow the steps for activating Okta.
 - a. The email address from the Welcome Message must be used. (Don't use an individual email address)
 - b. Set-up a password, security question and security image. Share this information with your usage reporting team.
2. When you download Google Authenticate and get to the "Scan Barcode" Step (Step 2 above), take a screen shot of the barcode. You can also select "can't scan" and copy the "Security Key"
 - a. The Bar Code /Security Key does not expire. It will be used by all team members
3. Complete the set-up.

4. Share the Bar Code or the Security Key number with your team.
5. All team members should download the Google Authenticator App and scan the bar code to access the authentication code for Data-Client Portal access.

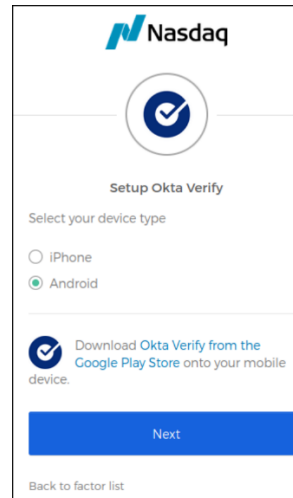
Using Okta Verify

Step 1

Select your mobile device.
You will be redirected to the Apple App Store for iPhones or Google Play for Androids.

Click "Next" and download the app.

Note: Set-up is the same for either type of device.

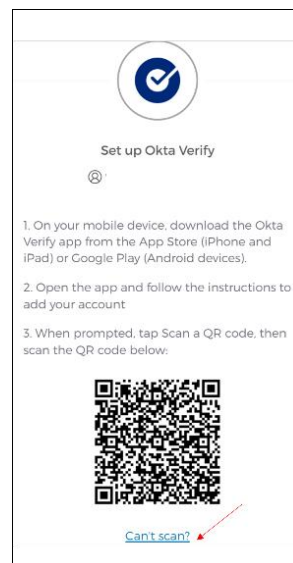


Step 2

After installing the application, open it and click on the "+" icon in the upper right corner (design may vary).

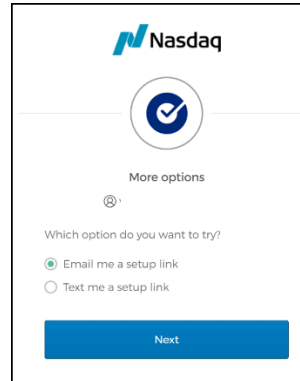
Once the QR code is scanned, your enrollment is complete.

If you cannot scan the QR code, click on "Can't scan?".



Select how you want to receive the log-in and click "Next." You will be prompted to enter your information.

Note: Email is recommended. The text option will disable push notifications for logins, reducing Verify functionality.

A screenshot of the Nasdaq login setup screen. At the top is the Nasdaq logo. Below it is a circular icon with a checkmark. The text "More options" is centered, followed by a small icon of a person. Below that is the question "Which option do you want to try?". There are two radio button options: "Email me a setup link" (which is selected) and "Text me a setup link". At the bottom is a blue button labeled "Next".

Nasdaq

More options

Which option do you want to try?

☒ Email me a setup link

☐ Text me a setup link

Next

Organizational Restrictions for External Applications

If your organization has firewall security policies about using an external application like OKTA, please discuss the requirements with your Information Technology (IT) division.

Options:

- Ask your IT division to "whitelist" signin@nasdaq.com.
- There are also instructions from Okta on setting up specific I.P. addresses. You can find those instructions [here](#).

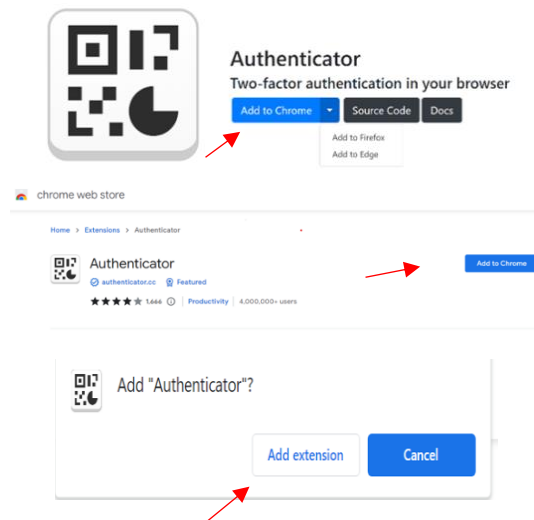
Using the Authenticator Extension

While it is recommended that a mobile phone be used to authenticate access, it is understandable that this may not be possible. As an alternative, you can upload the [Authenticator Extension](#) to your desktop. The extension may be used with Google Chrome, Microsoft Edge or the Firefox browser. Note: These instructions are for Google Chrome. Using the extension is very similar with the other browsers.

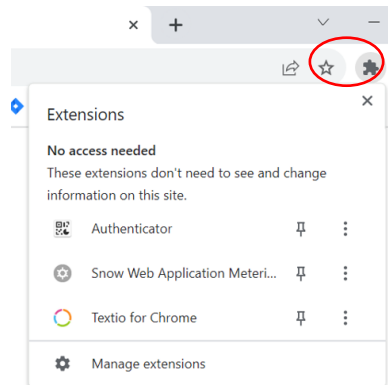
Step 1 Add the “Authenticator Extension” to your desktop.

Click on this link: [Authenticator Extension](#) in the Google Webstore and select the browser. You will be taken to the Chrome Web Store.

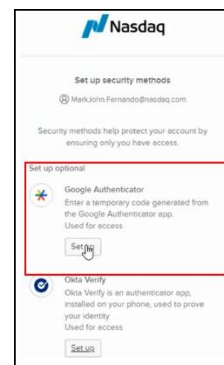
Click on “Add to <BROWSER SELECTED>”. Then click on “Add extension”



Click on this Puzzle Piece icon for the Extension



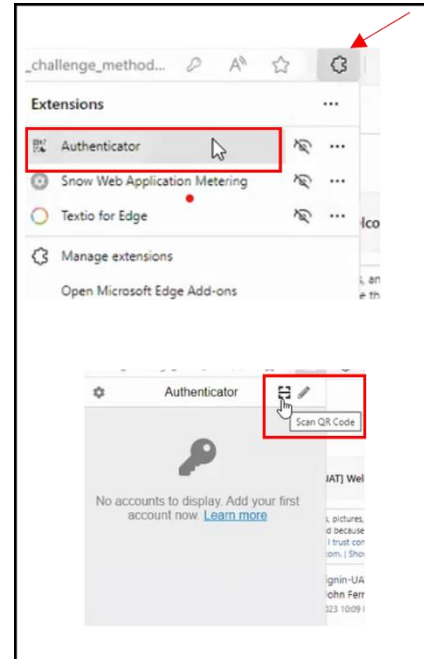
Step 2 Follow the steps beginning on Page 2 for the “Initial Set-up.” Select “Google Authenticator” as the Security Method.



You will be taken to the Bar Code.



Step 3 To scan the code, click on the "Puzzle Icon" and select "Authenticator."



You will see this message. Click on the "Scan QR Code" icon.

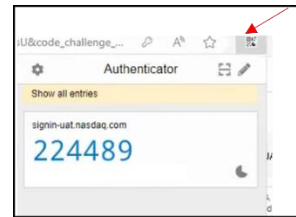
"Drag and Drop" the QR Code Click on the QR code box and hold your mouse button so that the entire QR Code is covered in the drag and drop selection box. Click on it.



A pop-up will confirm that it has been added. Click OK.



Click on the Authenticator (Puzzle Piece Icon) and it will show that an account has been added. This is where you will get the code when you log in.

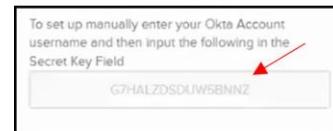


You are now set up to enter the code to access the Data-Client Portal.

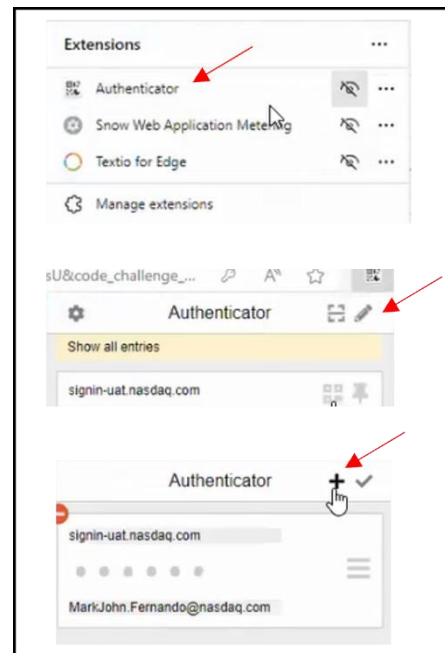
Part 4 If you cannot scan the QR code, click on "Can't Scan."



Copy the code.



Click on the Puzzle Piece Icon and select Authenticator.



Click on the pencil icon.

Click on the "Plus" sign.

Select Manual Entry

Issuer: signin.nasdaq.com

Enter "Secret" Code

Click on "Advanced" and enter your email.

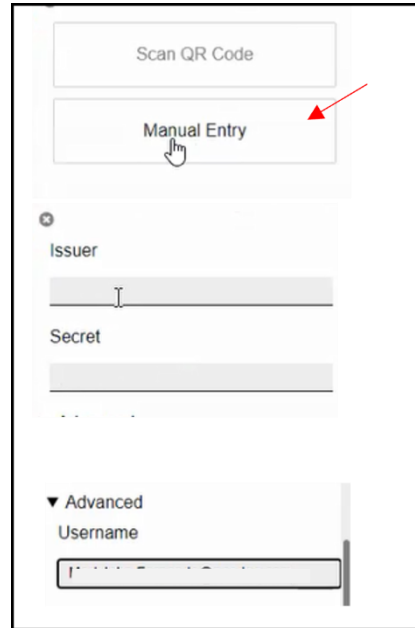
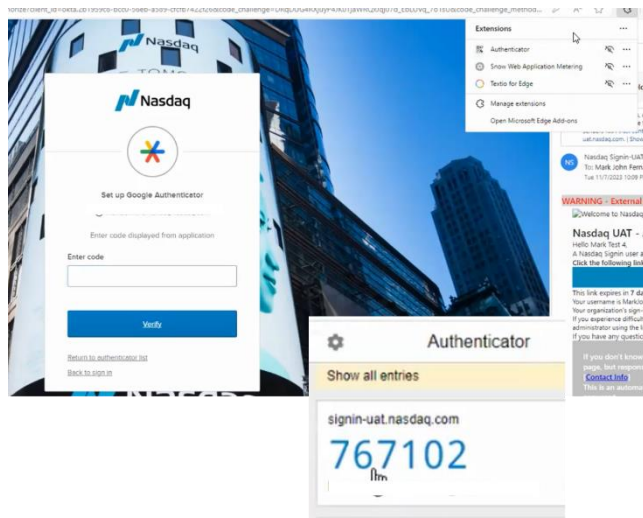
Click Next. You are now set up to enter the code to access the data-Client Portal.

Please note: You only need to scan the QR Code or enter it manually once.

When you want to access the Data-Client Portal, go to the Authenticator, and get the Code.

Enter the code when prompted.

Please note: The Code changes every 30 seconds.

Accessing Data-Client Portal for Usage Reporting

1. Go to Data-Client Portal: <https://nasdaq.screeninfomatch.com/Authentication/Login>
2. Click “Log in Here.” You will be redirected to Okta.
3. Enter User Name (email address) and password.
4. Okta Verify: Open the Okta Verify app and enter the six-digit code. Note this code refreshes every 30 seconds. If using a mobile device, select “Receive a Code via SMS”. The six-digit authentication code will be sent to your mobile device.
Google Authenticator: Go the the App for the six-digit authentication code.
Google Authenticator Extension: Go the Extension for the code.
5. Enter the authentication code. You will be redirected back to the Data-Client Portal.