DerivativePATH

Google Authticator

Access and Identity Management through Auth0

Google Authenticator Instructions

Here's how to set it up:

The first time you log into EDGE after the transition, there will be a **one-time setup** to link the authenticator of your choice to your profile.
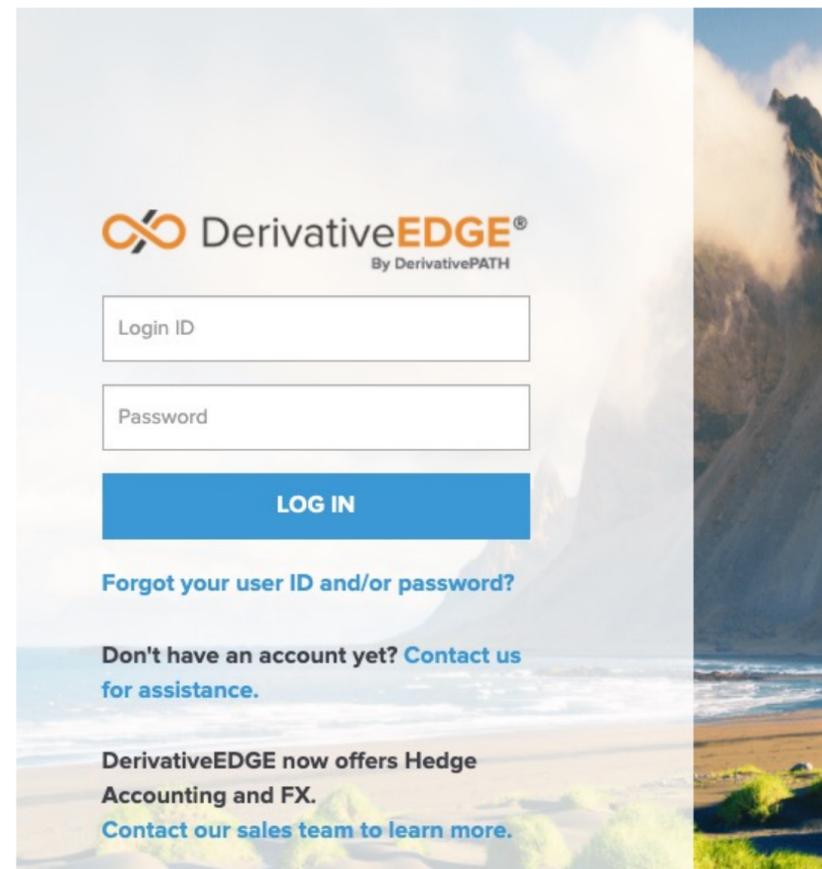
- Download the **Google Authenticator App**

  Download from either the **Apple App Store** [iOS] or the **Android Google Play Store** [Android]. It's free.
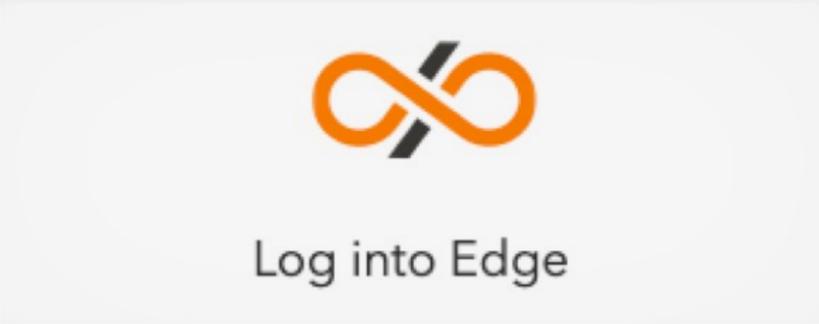

- Next, **Log in to EDGE** using your e-mail address and password.

  You will continue to use your current email and password to log in. For some users, they will be asked to change their passwords in the initial setup.

- Upon logging in, you will be taken to the authenticator selection screen. For Google Authenticator, click the "I'd rather use Google Authenticator" below.
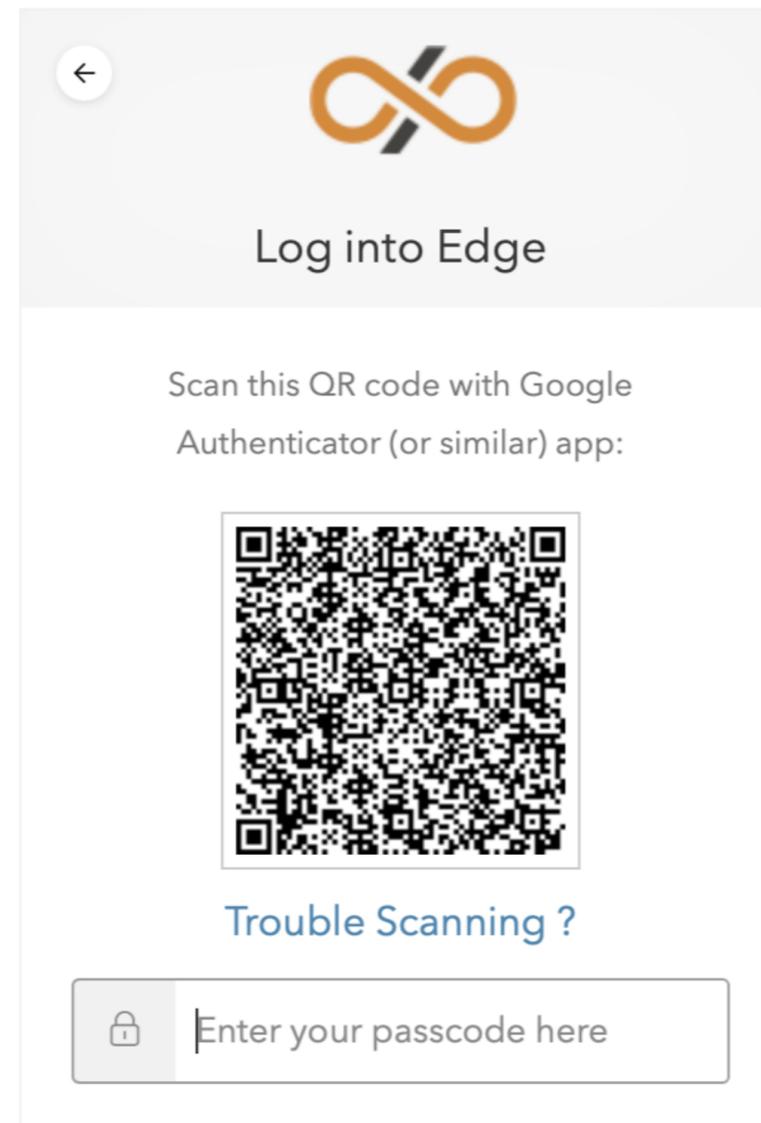
- Open the Google Authenticator app on your phone and tap the plus button

- From there, select "Scan a QR code" and scan the EDGE QR code with your phone's camera. This will automatically add the EDGE account to your authenticator app.

Scan a QR code

Enter a setup key
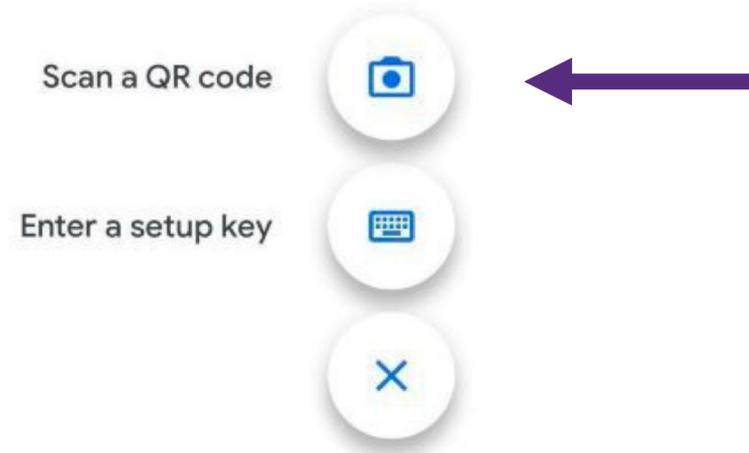
- Once you have scanned the code, back on EDGE, you will enter the six-digit code that appears on your app, where it says, "Enter your passcode here"

- If you can't scan a QR code or the app won't open correctly, click, "**Trouble Scanning?**"

Log into Edge

Scan this QR code with Google Authenticator (or similar) app:

Trouble Scanning ?

Enter your passcode here

- EDGE will provide you with a setup key. Go to the app and use the "Enter a setup key" option and enter it manually instead of pointing your phone at the QR code on your computer screen to verify Google Authenticator's connection with your account.

- Upon entering the code, via scanning or manual entry, you will be taken to a screen that has your recovery code. This is in case you lose your phone, or the authenticator app gets deleted. Write this down and remember to save EDGE's backup code somewhere safe, then click "I have safely recorded this code."
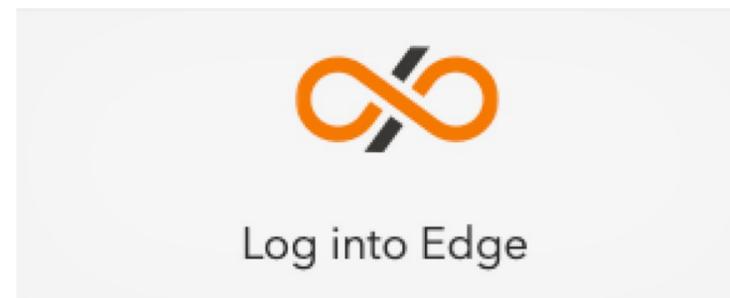

- Finally, you will receive a confirmation page that the authenticator setup is complete. Click Continue

Hot Tip

- The **next time you login to EDGE**, you will again be asked for the six-digit authentication code from your app. After providing, be sure to check the **"Remember this browser"** box when you login and EDGE will remember your browser for 30 days before prompting you for the code again.

DerivativeEDGE ®

January 2022 Access and Identity Management Re-Architecture FAQ

Why are these changes being made?

- Information security remains of the utmost importance to Derivative Path. The security landscape is constantly-shifting and these measures are designed to ensure the strictest safety of your data.

- The use of multi-factor security, password complexity algorithms and other protections are now considered standard protections in today's Access and Identity Management systems.

DerivativeEDGE ®

Access and Identity Management through Auth0

AIM is moving to Auth0

- **Auth0 is a Cloud-based Industry-leading solution** to managing user authentication

- **Customizable, extensible framework** supporting MFA, SSO (single sign on), universal login and other features

- **Heavily adopted** by the financial, insurance, and healthcare industries

**DerivativeEDGE®
Trading Platform**

**DerivativeEDGE® Branded
White Label FX**
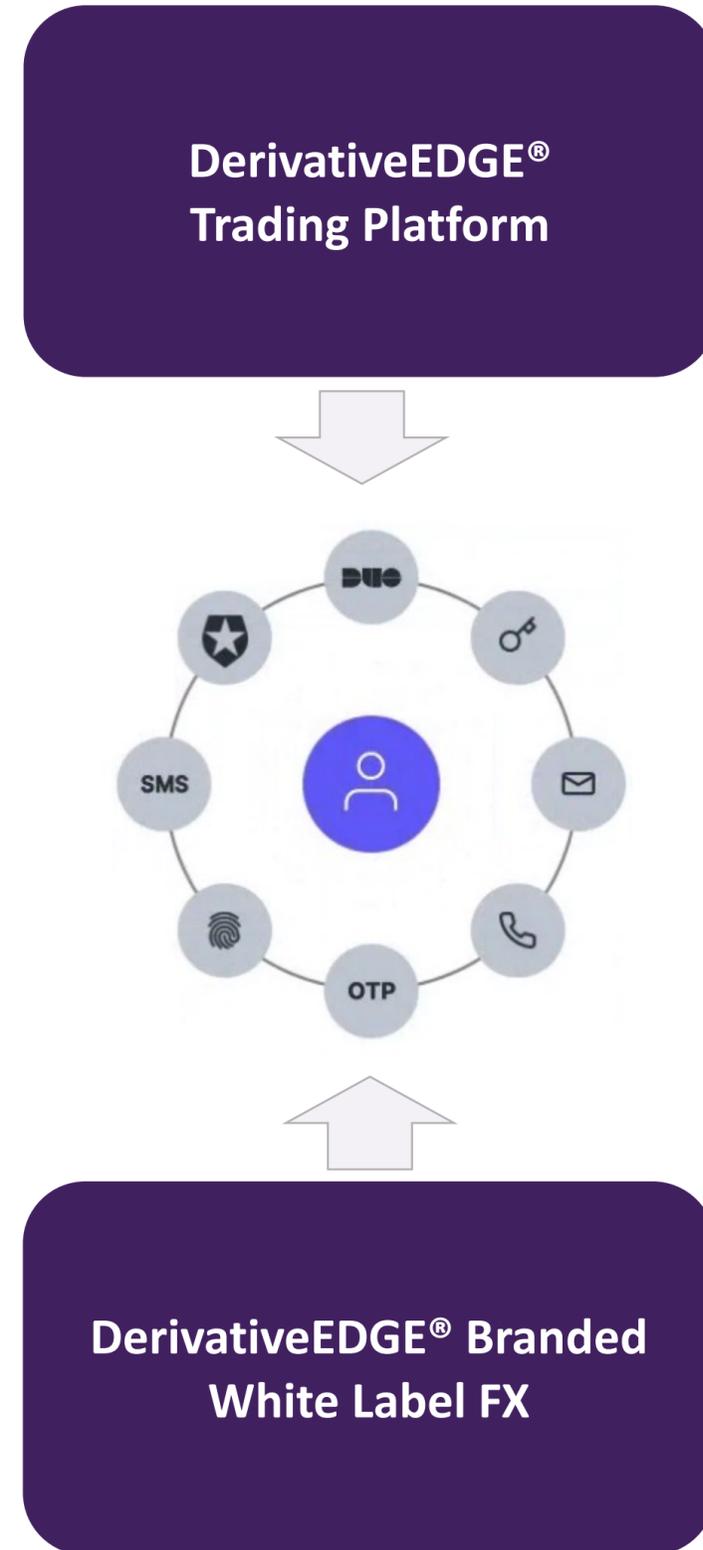
DerivativeEDGE ®

FAQ

Frequently Asked Questions

- Who do I contact for **support** if I have issues?

  Please contact support@derivativepath.com for any log-in related assistance.

- What if I **lose** or **replace** my phone which has my authenticator app for MFA?

  Derivative Path Support (or your internal AIM group if configured) can reset your MFA allowing you to re-enable it.

- Is there an advantage between Google Authenticator and Auth0 Guardian?
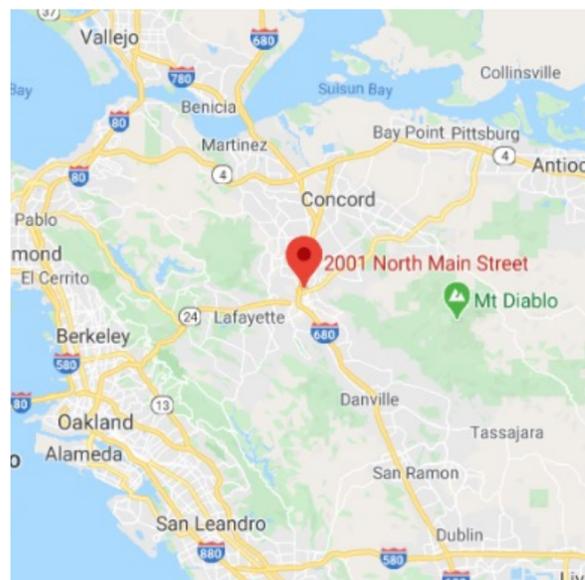
  Google Authenticator requires the app to be open on your phone and you key in a numeric code. Auth0 Guardian can send push notifications which some users may find easier to use.

- My **Information Security group** is asking if **SSO** will be enabled?

  SSO is on the product roadmap for 2022 but will not be enabled with the initial conversion.
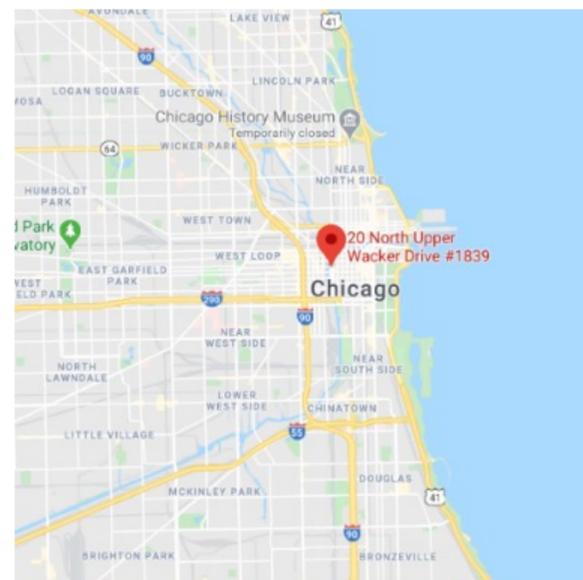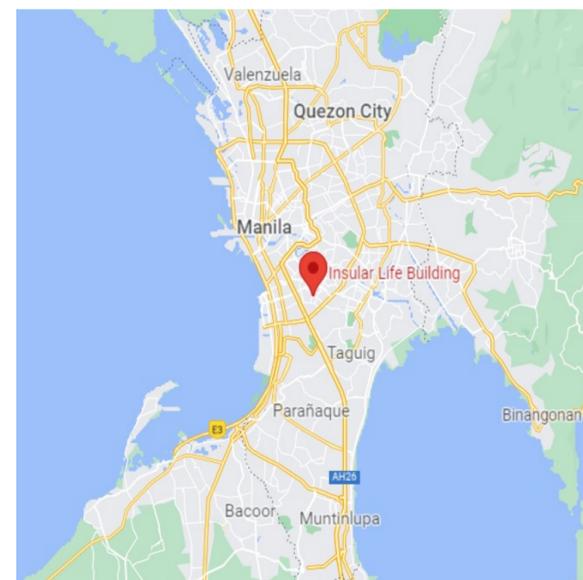
Disclosures

SAN FRANCISCO BAY AREA

NEW YORK CITY

CHICAGO

MANILA

General Risk Disclosure Statement
The Term "Derivative Path" refers to affiliates, Derivative Path, Inc. and Derivative Path Hedging Solutions. Inc.

Derivative Path, Inc. is headquartered in the State of California. Hedging advisory and execution services are provided through Derivative Path Hedging Solutions, Inc. (DPHS). DPHS is a Commodities Futures Trading Commission registered Introducing Broker and Commodity Trading Advisor and member of the National Futures Association.

This communication is for informational purposes only. It is not an offer, solicitation, recommendation, or commitment for any transaction or to buy or sell any security or other financial product and is not intended as investment advice or as a confirmation of any transaction.

This communication is intended as an information resource only. Derivative Path has taken reasonable measures to ensure the accuracy of this communication. Any information contained herein is not warranted as to completeness or accuracy, and Derivative Path accepts no liability for its use or to update or keep any such information current. These materials are confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed to any other party without the written consent of Derivative Path. All information contained herein is provided "as is" and may be subject to change without notice.