

Rockland Trust Investment Management Group enhanced login changes

MFA-multifactor authentication.

ROCKLAND
TRUST® Investment
Management Group

Rockland Trust Investment Management Group (IMG) customers will need to use Multi-Factor Authentication (MFA) in order to access their accounts online. This will be effective as of November 7, 2026.

Why is this change happening?

IMG's accounts are hosted on a platform called SEI. In an effort to continually guard against social engineering, phishing, and other Internet attacks, SEI is enhancing its Multi-Factor Authentication at account login.

What you need to know.

You will be required to enter your **User ID**, **Password** and a **One-Time PIN** every time you login. Question and Answers will be retired.

Phone number

You need to use your phone when logging in; an ID and password alone will not be enough. You will be asked to enter and verify a phone number that will be used to receive a text or voice call with your One-Time PIN during all future logins.

Authenticator app

Your site now supports using an authenticator app to obtain a **Time-Based One-Time PIN (TOTP)** instead of receiving the PIN as a text or voice call to your verified phone number. Its use is highly recommended for security purposes.

Forgot your password

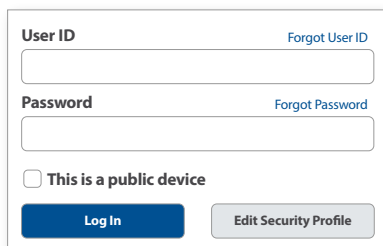
You must reset your password from the **Forgot Password** link on the login page; a verified phone number or authenticator app and email address are required. The IMG Team will not be able to reset passwords on your behalf.

How to Set Up MFA

Before November 7, navigate to the IMG login page.

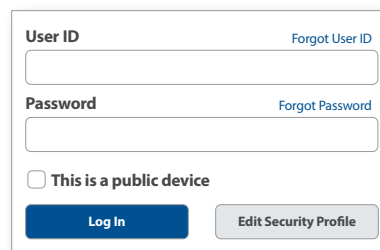
- 1 Enter **User ID** and **Password**, then click **Log In**

An email will be sent with a One-Time PIN



- 2 Enter the **One-Time PIN** from your email, then click **Continue**.
- 3 Enter your phone number and select your authentication method, then click **Continue**.
You will receive a text message or call with a One-Time PIN to enter.
- 4 Enter the **One-Time PIN** and click **Continue**

Subsequent login



Use this button to:

Change your password
Change your phone number
Add/Remove an authenticator application

- 1 Go to **<https://rocklandtrust.ecx.seic.com/>**
- 2 Enter **User ID** and **Password**, then click **Log In**
- 3 Select **authentication method** and click **Continue**
You will receive a text message or call with a One-Time PIN to enter. If you have an authenticator application set up, you will choose this method.
- 4 Enter the **One-Time PIN** from your text, call, or Authenticator Application and click **Continue**

The login process has been successfully completed. You'll now have access to the desired application.

Do not bookmark URLs.

A bookmark must contain the actual URL desired and not the redirected URL that is displayed with the login page. When adding a new bookmark or favorite, type the full url: **<https://rocklandtrust.ecx.seic.com/>**

Authenticator Application

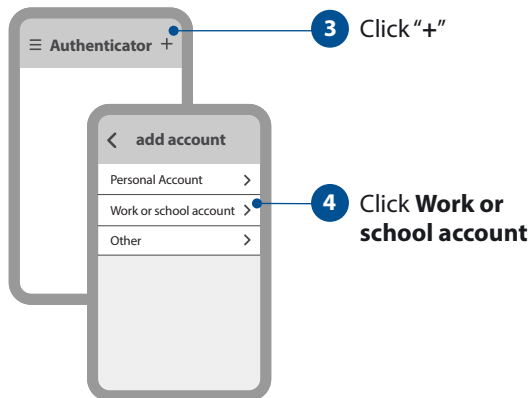
About authenticator applications

- Typically found on a mobile device.
- Provides a **Time-Based One-Time PIN (TOTP)** to enter into the MFA UI. It is usually valid for **30 seconds**.
- Similar to getting an OTP from a phone, but is more secure and quicker because it does not require any network connectivity between your device and the SEI system.
- SEI MFA will generate a QR code which you can scan with your mobile device.
- The authenticator app will store that secret key and give a user a 6-digit number which is typed into the MFA page. Once setup, this method can then be used to enter OTPs during login.
- If the authenticator app is deleted, a new mobile device is used, or a new version of the app has been installed, you will need to follow the initial setup instructions again.

Setup

- 1 Download and install an Authenticator application on your device. Popular choices are **Microsoft Authenticator** or **Google Authenticator**.

- 2 Open app on your device



- 5 From the IMG login screen, enter User ID and Password, then click Edit Security Profile.

User ID [Forgot User ID](#)

Password [Forgot Password](#)

☐ This is a public device

[Log In](#) [Edit Security Profile](#)

Use this button to:

Change your password
Change your phone number
Add an authenticator application

- 6 Select **authentication method** and click **Continue**
You will receive a text message or call with a One-Time PIN to enter. If you have an authenticator application set up, you will choose this method.

- 7 Enter the **One-Time PIN** and click **Continue**

- 8 Select **Set Up an Authenticator Application**, then click Proceed

Security Profile

User ID: UserID1 [Edit](#)

Password: ***** [Edit](#)

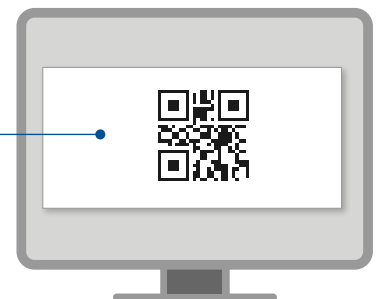
Email: email@co.com [Edit](#)

Phone: 1-111-111-1111 [Edit](#)

[Set Up an Authenticator Application](#)

[Proceed](#)

- 9 Scan **QR Code** with your mobile device from your computer screen



Be sure to scan the QR code from within the Authenticator App, NOT from your device's camera.

- 10 Enter the **TOTP** received via Authenticator App
TOTP is usually valid for 30 seconds

Enter the Timed-Based One-Time PIN that was sent to your Authenticator Application.

Resend One-Time PIN

[Continue](#) [Cancel](#)

If this OTP is not entered, the Authenticator will not be available, but will appear on the Edit Security page.