Multi-Factor Authentication (MFA) Requirement for GiveSmart Admin Access

Last Modified on 06/05/2026 3:41 pm EDT

Overview

To strengthen account security and provide a more consistent login experience across products, **Momentive Identity now requires Multi-Factor Authentication (MFA)** for all clients using:

- **Email One-Time Passcode (OTP)**

This update ensures that all administrative users accessing GiveSmart and related platforms are protected by an additional layer of security.

Why This Change Is Being Made

- Improve overall account security
- Deliver a consistent login experience across products
- Reducing risk of unauthorized access

What This Means for Your Organization

Once MFA is enabled for your organization:

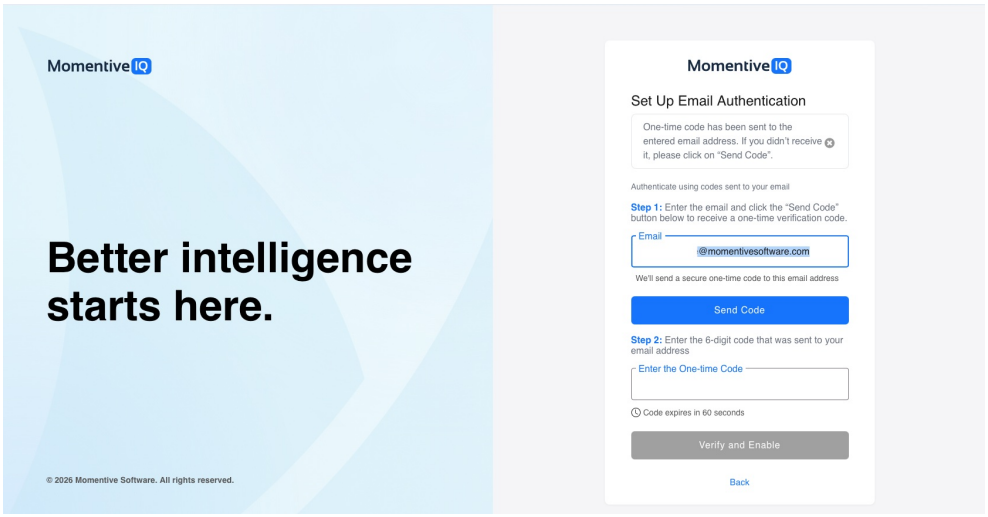
- All administrators with **Momentive user permissions** will be required to set up MFA
- This is enforced at the **organization level**, ensuring consistent protection across products
- Each admin will complete a **one-time setup during login**

How MFA Setup Works (Step-by-Step)

When signing in after MFA is enabled, administrators will be guided through a quick setup:

Step 1: Verify Email Address

- Confirm or enter the email address where you would like to receive verification codes
- Select **Send Code**

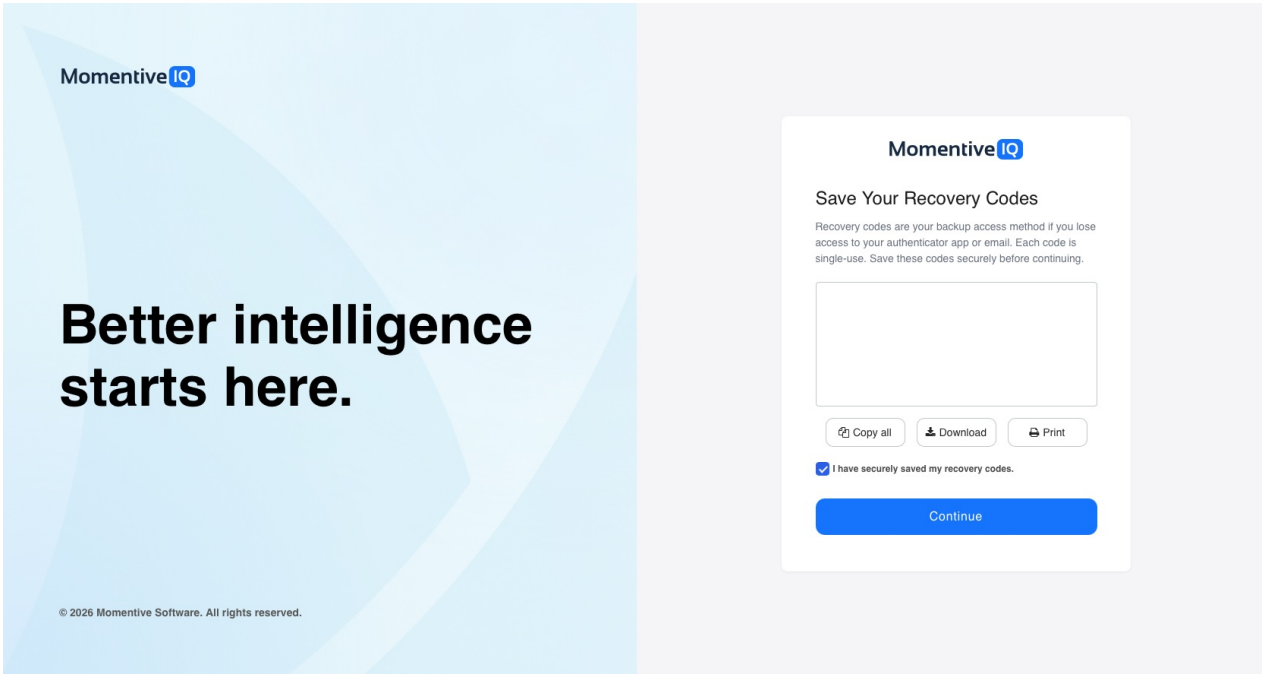


Step 2: Enter Verification Code

- Check your email inbox
- Enter the **6-digit code** sent to your email

Step 3: Save Recovery Codes

- You will be provided with> **recovery codes**
- Save these securely (recommended: password manager or secure document storage)
- Confirm you have saved them, then select **Continue**



IMPORTANT NOTES:
(1) Recovery codes are critical: They allow you to regain access if you cannot access your email or authenticator.
(2) Each administrator must complete their own setup.
(3) This process typically takes only a few minutes.

After Setup

Once MFA setup is complete:

- Your login will be successfully completed
- You can proceed to access and manage your **GiveSmart modules** as usual
- MFA will be required for future logins to ensure ongoing security

---

Important Notes

- **Recovery codes are critical**: They allow you to regain access if you cannot access your email or authenticator
- Each administrator must complete their own setup
- This process typically takes only a few minutes

FAQS

Who is impacted by this change?

All administrators with Momentive user permissions must use MFA.
This does **not impact donors or lower admin users**.

Can we opt out of MFA?

No. This is a platform-level security requirement to ensure all organizations are consistently protected.

Will this disrupt our workflow?

- Initial setup: quick, one-time step
- Ongoing: minimal impact (entering a verification code at login)

What happens if an admin doesn't complete setup?

They will not be able to proceed with login until MFA is configured.

What is the code length?

- MFA codes are **6 digits**

How long is the verification code valid?

- **Email OTP:** valid for **60 seconds**
- If the code expires, a new one can be requested or will refresh automatically (for authenticator apps).

How long does MFA verification last after login?

Once you successfully enter your code:

- The verification session remains valid for **5 minutes**
- This allows enough time to complete login without needing to re-enter the code.

What does “Trust this device” mean?

When you select **“Trust this device”**:

- You will not be prompted for MFA on that device for **30 days**
- This reduces friction for frequently used, secure devices
- Only use this option on **trusted, personal or work devices**

What if someone gets locked out?

- First, try using recovery codes
- If unavailable, contact GiveSmart Support