CIRCULAR 084-26
June 17, 2026

MX-R CONNECT - ENABLING OF MULTI-FACTOR AUTHENTICATION

The Regulatory Division advises Approved Participants that multi-factor authentication ("MFA") will be enabled for its participant portal, MX-R Connect, effective **July 6, 2026**.

Impact on MX-R Connect users

Users will be required to authenticate from an additional factor in order to login to MX-R Connect. Please refer to Appendix A for alternatives and questions.

In addition, users may no longer be able to login from a shared account. Please contact your community administrator to have your own user account created.

For more information or for any questions, please contact the Regulatory Division:

- mxr-connect@tmx.com
- 514-787-6530
- Toll-free from Canada and US: 1-800-361-5353 extension 46530
- Toll-free from the UK and France: 00 800 36 15 35 35 extension 46530

John Cambareri
Interim President, Regulatory Division of Montréal Exchange Inc.

Appendix A: MX-R Connect with Multi-Factor Authentication

As we enhance security around our Participant Portal, MX-R Connect is introducing **Multi-Factor Authentication ("MFA")**. MFA adds an extra layer of protection to your account by requiring two forms of verification when you log in: something you know (your password) and something you have (a mobile device).

This guide will walk you through how MFA works, what apps you can use, and how to set it up.

How It Works

Once MFA is enabled, logging into MX-R Connect will become a simple two-step process:

1. **Enter your credentials:** Type in your username and password as you normally do
2. **Verify your identity:** Approve a login request on your mobile device or enter a 6-digit verification code from an authenticator app

Supported Authenticator Apps

Option 1: Salesforce Authenticator (Highly Recommended)

We strongly encourage using the Salesforce Authenticator app. It is specifically designed to make logging in as seamless as possible.

- **Push Notifications:** Instead of typing in a 6-digit code, you simply tap **"Approve"** on a push notification that pops up on your phone
- **Trusted Locations:** You can set the app to automatically verify your identity when you are logging in from a trusted location (like your home or office Wi-Fi), saving you a step
- **Free to Use:** Available for both iOS and Android
- For a detailed, step-by-step visual guide on setting up and using Salesforce Authenticator, please review the official usage video: Get Started with Salesforce Authenticator

Option 2: TOTP Authenticator Apps

If you prefer, you can use any third-party app that supports Time-based One-Time Passwords (TOTP / RFC 6238). These apps generate a new 6-digit code every 30 seconds, which you will type into MX-R Connect during login. Popular options include:

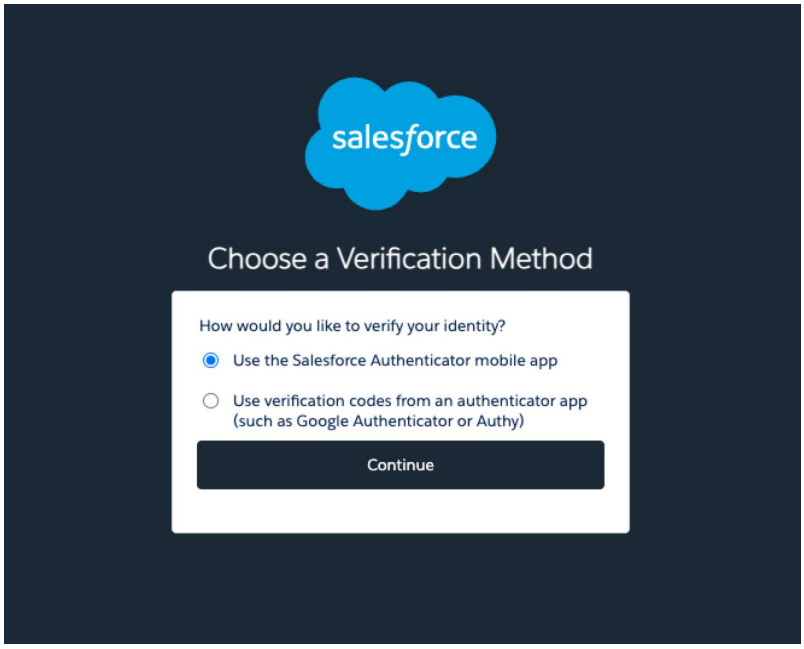
- **Google Authenticator**
- **Microsoft Authenticator**

- **Authy**
- **Aegis Authenticator (Open Source)**
- **Many modern password managers also have TOTP functionality built in**

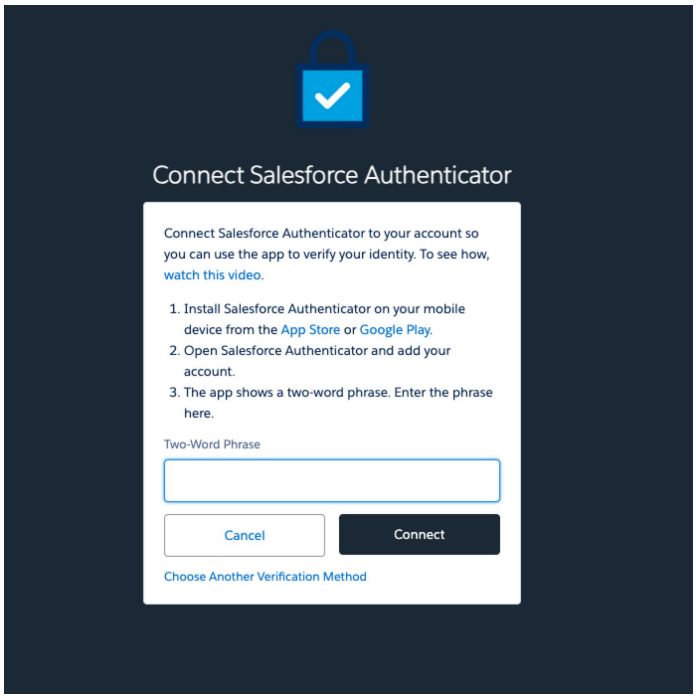
Step-by-Step Setup Guide

You will only need to complete this setup process once.

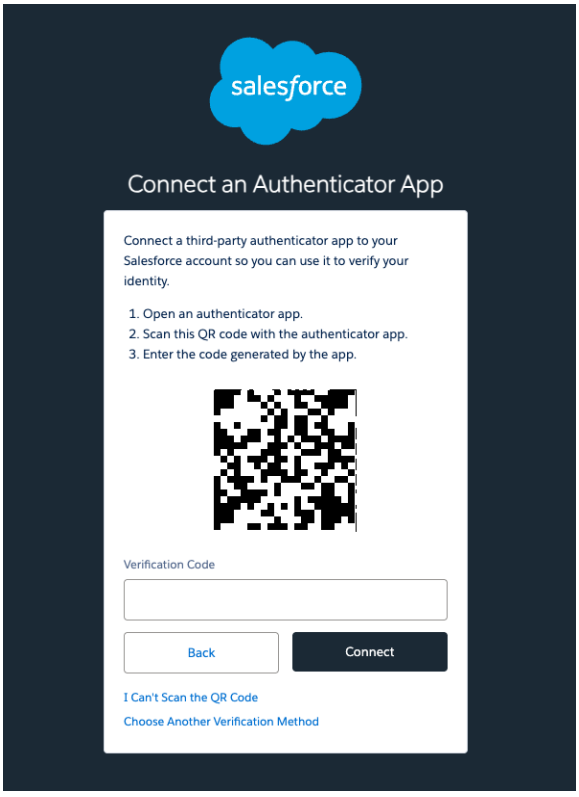
1. **Download an App:** Download either **Salesforce Authenticator** or your preferred TOTP app from the Apple App Store or Google Play Store.
2. **Log into MX-R Connect:** Enter your username and password. You will automatically be prompted to connect an authenticator app.



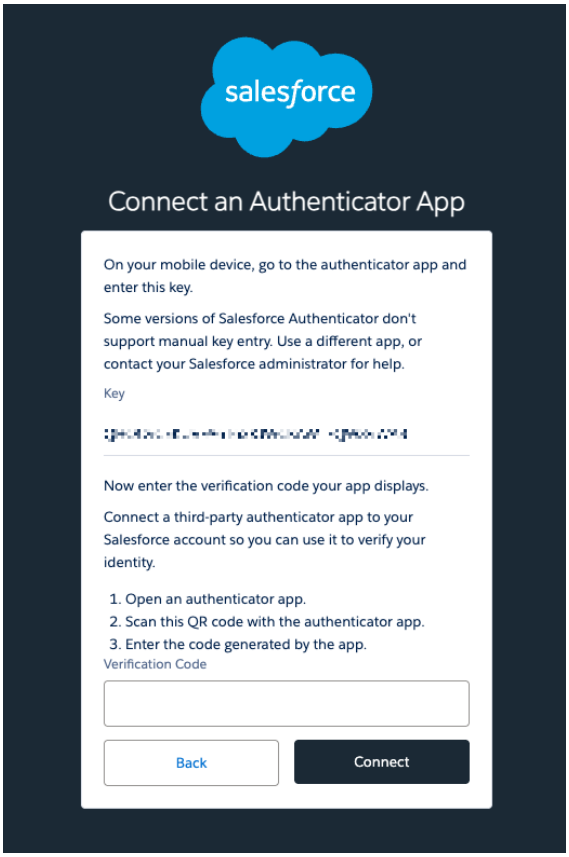
3. **Connect Your App:**
    - **If using Salesforce Authenticator:** Open the app on your phone, tap **Add an Account**, and a unique two-word phrase will appear. Type that phrase into the MX-R Connect prompt on your computer screen and click **Connect**.



- **If using a TOTP App:** Click the link on your screen that says "**Use a different authenticator app**". Open your app, choose to add a new account, and scan the QR code displayed on your screen. Type in the 6-digit code it generates to confirm.



- If you're using an Authenticator App where you don't have access to a camera to scan the QR code, please click "**I Can't Scan the QR Code**" and follow the instructions. This will require you to copy and paste a key across to your authentication app of choice.



4. **Complete Login:** Once connected, you will be securely logged into MX-R Connect.

Frequently Asked Questions (FAQ)

What is Multi-Factor Authentication (MFA), and why is it required?

Multi-Factor Authentication (MFA) requires two distinct forms of identification to access your account. This additional layer of security protects your data from unauthorized access, even in the event of a compromised password.

Can I receive a verification code via text message (SMS) or email instead?

No. SMS and email verification methods are increasingly susceptible to interception. Authenticator apps provide a significantly higher level of encryption and security, aligning with modern industry standards for protecting user data.

Will I be prompted for MFA during every login attempt?

Yes. However, if you utilize the Salesforce Authenticator app, you have the option to enable trusted locations. This feature automatically verifies your identity when logging in from a recognized network (such as your standard home or office Wi-Fi) or location. If you use a standard TOTP app (e.g. Google or Microsoft Authenticator), you will be required to enter a 6-digit code for each session.

Am I required to use a smartphone app?

No, you may use any application that supports Time-based One-Time Passwords (TOTP). This includes smartphone apps, desktop applications, browser extensions, and many modern enterprise password managers. If your organization has a preferred or mandated authentication application, please use that designated tool. We recommend consulting with your internal IT or Security team for guidance on the best application to use.

What is the procedure if I lose my device or acquire a new one?

If you lose access to your authenticated device, please contact our support team at mxr-connect@tmx.com. An administrator will securely clear your existing MFA profile, allowing you to register a new device during your next login attempt.

What should I do if I receive an unexpected login approval request?

If your authenticator app prompts you for an approval or generates a notification while you are not actively attempting to log into MX-R Connect, **deny the request immediately and contact us as soon as possible**. This indicates an unauthorized attempt to access your account. After denying the request, please login and reset your MX-R Connect account password as a precautionary measure.

Who do I contact for technical assistance during setup?

If you encounter any difficulties while registering your authenticator app, please contact our support team at mxr-connect@tmx.com.