CIRCULAIRE 084-26
Le 17 juin 2026

MX-R CONNECT – ACTIVATION DE L'AUTHENTIFICATION MULTIFACTEUR

La Division de la Réglementation informe les Participants Agréés que l'authentification multifacteur sera activée sur son portail des participants, MX-R Connect, à compter du **6 juillet 2026**.

Incidence sur les utilisateurs de MX-R Connect

Les utilisateurs devront fournir un facteur de validation supplémentaire afin d'ouvrir une session dans MX-R Connect. Veuillez-vous reporter à l'annexe A pour connaître les solutions de rechange et formuler vos questions.

Par ailleurs, il se pourrait que les utilisateurs ne puissent plus se connecter à partir d'un compte partagé. Veuillez communiquer avec votre administrateur communautaire afin de procéder à la création de votre propre compte d'utilisateur.

Pour toute question, veuillez communiquer avec la Division de la Réglementation :

- mxr-connect@tmx.com
- 514 787-6530
- Sans frais au Canada et aux États-Unis : 1 800 361-5353, poste 46530
- Sans frais au Royaume-Uni et en France : 00 800 36 15 35 35, poste 46530

John Cambareri
Président par intérim, Division de la Réglementation de Bourse de Montréal Inc.

Annexe A : Ajout de l'authentification multifacteur à MX-R Connect

Afin de rehausser la sécurité de notre portail des participants, la plateforme MX-R Connect intègre désormais l'**authentification multifacteur (« AMF »).** L'AMF ajoute un degré de protection supérieur à votre compte en exigeant deux modes de validation lors de la connexion : votre mot de passe (que seul vous connaissez) et l'appareil mobile que vous possédez.

Ce guide vous présente le fonctionnement de l'AMF, les applications compatibles et la marche à suivre pour la configurer.

Fonctionnement

Une fois l'AMF activée, la connexion à MX-R Connect se fait en deux étapes simples :

1. **Entrez vos identifiants :** saisissez votre nom d'utilisateur et votre mot de passe comme vous le faites d'habitude.
2. **Vérifiez votre identité :** approuvez la demande de connexion sur votre appareil mobile ou saisissez le code de vérification à 6 chiffres généré par une application d'authentification.

Applications d'authentification prises en charge

Option 1 : Salesforce Authenticator (fortement recommandé)

Nous vous recommandons fortement d'utiliser l'application Salesforce Authenticator. Elle a été spécialement conçue pour rendre la connexion aussi simple et fluide que possible.

- **Notifications poussées :** Au lieu de saisir un code à 6 chiffres, il vous suffit d'appuyer sur « **Approuver** » dans la notification poussée qui s'affiche sur votre téléphone.
- **Lieux de confiance :** Vous pouvez configurer l'application pour qu'elle valide automatiquement votre identité lorsque vous vous connectez à partir d'un emplacement de confiance (comme le réseau Wi-Fi de votre domicile ou de votre bureau), ce qui vous épargne une étape.
- **Gratuit :** disponible pour iOS et Android
- Pour obtenir une présentation visuelle détaillée de la configuration et de l'utilisation de Salesforce Authenticator, veuillez visionner le tutoriel vidéo officiel : Premiers pas avec Salesforce Authenticator *(Get Started with Salesforce Authenticator)* en anglais

Option 2 : Applications d’authentification à mot de passe dynamique temporel

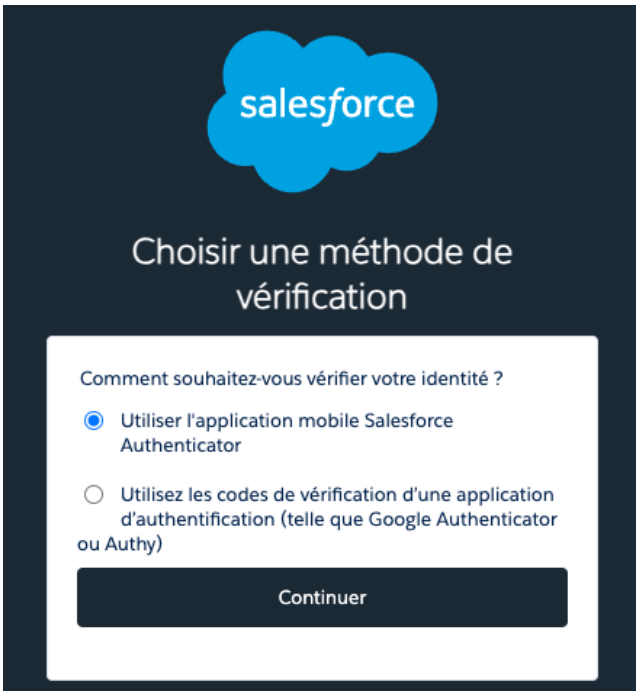
Si vous le souhaitez, vous pouvez utiliser n’importe quelle application tierce qui utilise les mots de passe dynamiques temporels (TOTP / RFC 6238). Ces applications génèrent un nouveau code à 6 chiffres chaque 30 secondes, que vous devez saisir dans MX-R Connect au moment de vous connecter. Options courantes :

- **Google Authenticator**
- **Microsoft Authenticator**
- **Authy**
- **Aegis Authenticator (Open Source)**
- **De nombreux gestionnaires de mots de passe actuels intègrent également la fonctionnalité de mot de passe dynamique temporel**

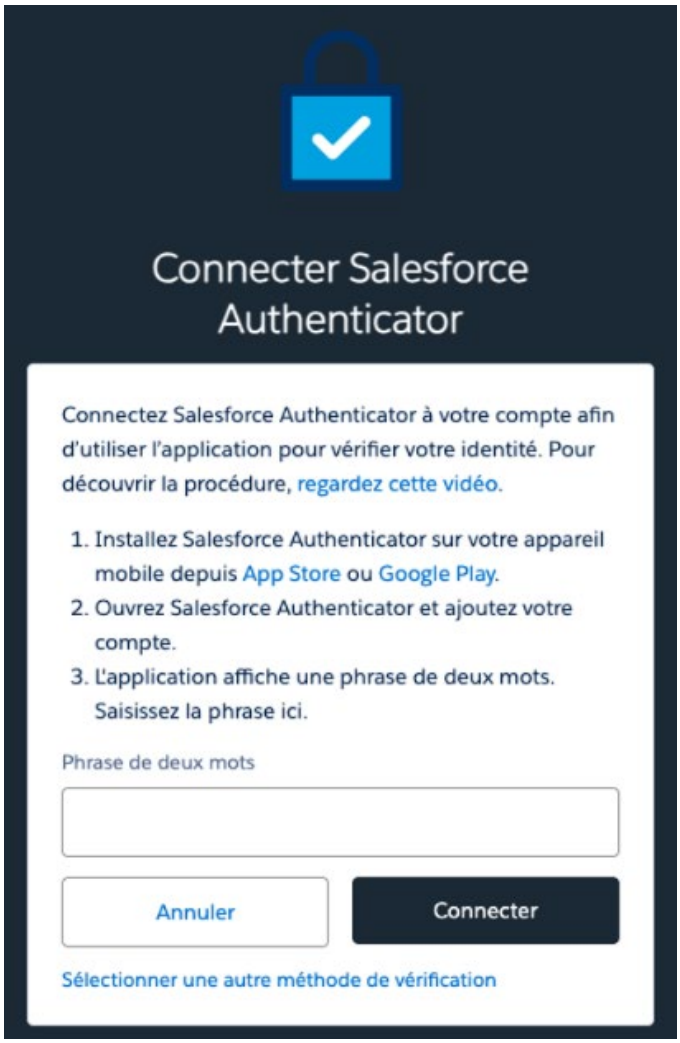
Guide de configuration étape par étape

Vous n’aurez à effectuer cette configuration qu’une seule fois.

1. **Téléchargez une application :** téléchargez soit **Salesforce Authenticator**, soit l’application de mot de passe dynamique temporel de votre choix depuis l’App Store d’Apple ou le Google Play Store.
2. **Ouvrez une session dans MX-R Connect :** Entrez votre nom d’utilisateur et votre mot de passe. Vous serez automatiquement invité à lier une application d’authentification.



3. **Liez votre application :**
    - **Si vous utilisez Salesforce Authenticator :** Ouvrez l'application sur votre téléphone, appuyez sur **Ajouter un compte**, et une phrase unique de deux mots s'affichera. Saisissez cette phrase dans le champ de saisie de MX-R Connect sur l'écran de votre ordinateur, puis cliquez sur **Connecter**.



    - **Si vous utilisez une application de mot de passe dynamique temporel :** Cliquez sur le lien à l'écran qui indique **Sélectionner une autre méthode de vérification.** Ouvrez votre application, choisissez d'ajouter un nouveau compte, puis numérisez le code QR affiché à l'écran. Saisissez le code à 6 chiffres généré par l'application pour confirmer.

- Si vous utilisez une application d'authentification et que vous n'avez pas accès à un appareil photo pour numériser le code QR, veuillez cliquer sur **Je ne peux pas numériser le code QR** et suivre les instructions. Vous devrez alors copier une clé et la coller dans l'application d'authentification de votre choix.

4. **Terminer la connexion :** une fois la connexion établie, vous serez connecté de manière sécurisée à MX-R Connect.

Foire aux questions (FAQ)

Qu'est-ce que l'authentification multifacteur et pourquoi est-elle obligatoire?

L'authentification multifacteur prévoit deux modes d'identification distincts pour accéder à votre compte. Ce niveau de sécurité supplémentaire protège vos données contre les accès non autorisés, même en cas de mise à découvert de votre mot de passe.

Puis-je plutôt recevoir un code de vérification par message texte ou par courriel?

Non. Les méthodes de vérification par message texte et par courriel sont de plus en plus vulnérables aux interceptions. Les applications d'authentification offrent un niveau de chiffrement et de sécurité nettement supérieur, s'alignant ainsi sur les normes actuelles du secteur en matière de protection des données d'utilisateur.

Est-ce que l'authentification multifacteur me sera demandée pour chaque tentative de connexion?

Oui. Cependant, si vous utilisez l'application Salesforce Authenticator, vous avez la possibilité d'activer des lieux de confiance. Cette fonctionnalité valide automatiquement votre identité lorsque vous vous connectez à partir d'un lieu ou d'un réseau reconnu (comme le réseau Wi-Fi de votre domicile ou de votre bureau). Si vous utilisez une application de mot de passe dynamique temporel standard (comme Google Authenticator et Microsoft Authenticator), vous devrez saisir un code à 6 chiffres lors de chaque ouverture de session.

Suis-je tenu d'utiliser une application pour téléphone intelligent?

Non, vous pouvez utiliser n'importe quelle application qui prend en charge les mots de passe dynamiques temporels. Cela comprend les applications pour téléphone intelligent, les logiciels de bureau, les extensions de navigateur et de nombreux gestionnaires de mots de passe d'entreprise actuels. Si votre organisation privilégie ou impose une application d'authentification particulière, veuillez utiliser l'outil ainsi désigné. Nous vous recommandons de consulter votre équipe des TI ou de sécurité interne afin d'obtenir des conseils sur la meilleure application à utiliser.

Que dois-je faire si je perds mon appareil ou si j'en obtiens un nouveau?

Si vous perdez l'accès à votre appareil d'authentification, veuillez communiquer avec notre équipe de soutien à l'adresse mxr-connect@tmx.com. Un administrateur réinitialisera votre profil d'authentification multifacteur en toute sécurité, ce qui vous permettra d'enregistrer un nouvel appareil lors de votre prochaine tentative de connexion.

Que dois-je faire si je reçois une demande inhabituelle d'approbation de connexion?

Si votre application d'authentification vous envoie une demande d'approbation ou génère une notification alors que vous n'essayez pas de vous connecter à MX-R Connect, **refusez la demande immédiatement et communiquez avec nous dès que possible.** Cela indique une tentative d'accès non autorisée à votre compte. Après avoir refusé la demande, veuillez ouvrir une session et réinitialiser le mot de passe de votre compte MX-R Connect par mesure de précaution.

Avec qui dois-je communiquer pour obtenir de l’assistance technique lors de la configuration?

Si vous avez de la difficulté à configurer votre application d’authentification, veuillez communiquer avec notre équipe de soutien à l’adresse mxr-connect@tmx.com.