

Authentification multifactorielle avec Microsoft Entra ID

Processus d'inscription utilisant un appareil mobile IOS

**Guide de
l'utilisateur
externe et
FAQ**

Contenu

Objectifs et conditions préalables	2
Participer au déploiement de l'inscription à l'authentification multifactorielle	2
Authentification multifactorielle pour les options mobiles	3
Avez-vous reçu l'invitation de vous inscrire de Metrolinx?	4
Accepter votre invitation à vous inscrire	5
S'inscrire avec l'application Authenticator (Option A)	8
Inscrivez-vous par SMS ou téléphone (Option B)	13
Inscrire des méthodes supplémentaires pour l'authentification multifactorielle (facultatif)	15
FOIRE AUX QUESTIONS (FAQ) : Foire aux questions	16
QUESTIONS GÉNÉRALES	16
QUESTIONS RELATIVES À L'INSCRIPTION	18

Objectifs et conditions préalables

Ce guide vous guide dans le processus d'inscription à l'authentification multifactorielle pour les utilisateurs qui accèdent aux ressources de Metrolinx en utilisant un **compte non Metrolinx**, y compris les trois options disponibles (voir le tableau résumant les options à la page 2).

Pour compléter ce processus, vous devrez avoir :

- Un appareil mobile IOS
 - Si vous utilisez un appareil mobile Android, consultez le Guide d'inscription à l'authentification multifactorielle pour les appareils Android.
- un courriel d'invitation pour s'inscrire à l'authentification multifactorielle
deinvites@metrolinx.onmicrosoft.com
 - Si vous n'avez pas reçu d'invitation par courriel, vérifiez votre dossier des courriers indésirables avant de contacter le service de dépannage.

Si vous rencontrez des difficultés à vous inscrire à l'authentification multifactorielle, vous pouvez contacter le service de dépannage pour obtenir de l'aide au numéro : 416-202-5000 (option 3 du répertoire)

Participer au déploiement de l'inscription à l'authentification multifactorielle

À partir de décembre 2025, Metrolinx a commencé à déployer l'authentification unique et l'authentification multifactorielle utilisant Microsoft Entra ID pour accéder aux applications Oracle suivantes à compter du 30 mars 2026 : iSupplier, Oracle Primavera Unifier et Oracle Aconex.

Si vous participez à ce déploiement, vous aurez reçu un courriel de [SSO MFA EntraID@Metrolinx.com](mailto:SSO_MFA_EntraID@Metrolinx.com), faisant référence au présent Guide pour savoir comment enregistrer votre compte pour l'authentification multifactorielle chez Metrolinx.

Veuillez suivre les instructions ci-dessous pour compléter l'enregistrement de votre compte et contribuer à mieux sécuriser les actifs numériques de Metrolinx.

Authentification multifactorielle pour les options mobiles

Au cours du processus d'inscription, il vous sera demandé de sélectionner une option d'authentification multifactorielle. Le tableau ci-dessous résume vos options. Une fois que vous avez décidé de l'option pour vous inscrire, veuillez passer à la section appropriée à la page 5.

Option	Renseignements	Recommandé à...
A Microsoft Authenticator	***Option recommandée*** - Nécessite un appareil mobile intelligent avec iOS 16.0 ou une version ultérieure* - Nécessite le téléchargement de l'application Microsoft Authenticator	- Utilisateurs qui possèdent un appareil mobile intelligent - Utilisateurs qui souhaitent inscrire plusieurs appareils
B Téléphone (code à usage unique envoyé par SMS ou par appel vocal)	- Ne nécessite pas un appareil mobile intelligent* (compatible avec les appareils mobiles plus anciens) - Nécessite une connexion à un réseau mobile (c.-à-d., ne fonctionnera PAS en mode Avion)	Utilisateurs qui ne possèdent pas d'appareil mobile intelligent*

**Un appareil mobile intelligent a accès à Internet et peut télécharger des applications.*

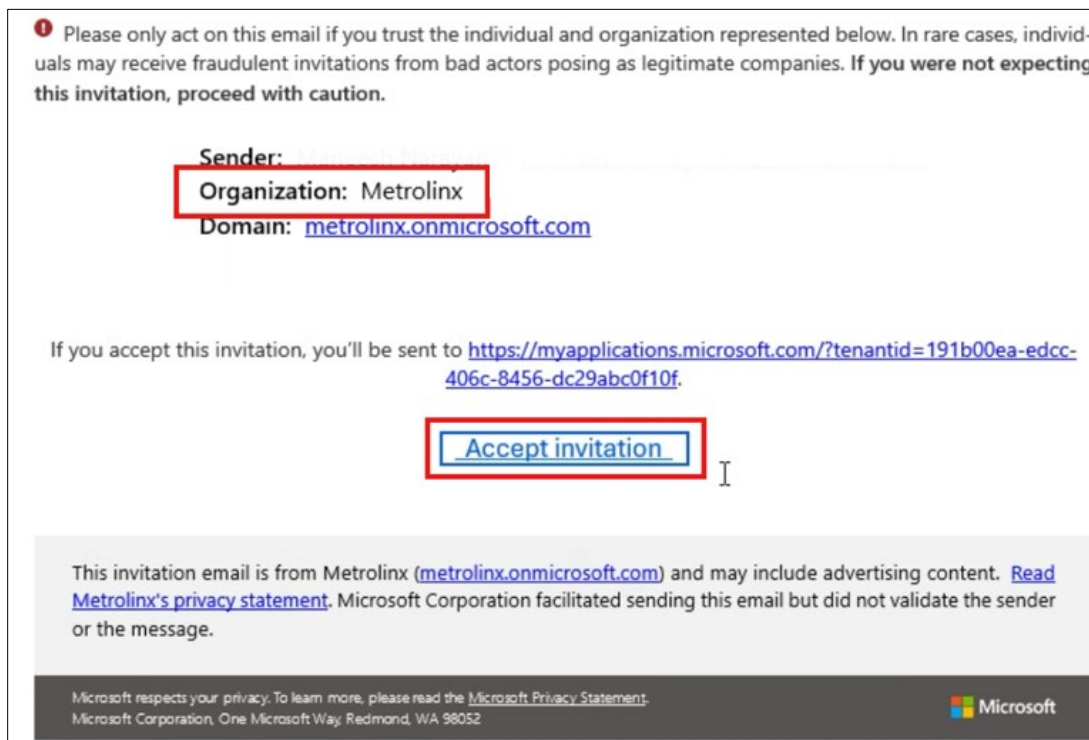
Nous recommandons d'enregistrer les deux options d'authentification multifactorielle afin de prévenir les interruptions de connexion futures et de minimiser le besoin d'aide au service d'assistance dans les cas où une méthode spécifique d'authentification multifactorielle n'est pas disponible. Par exemple, si vous mettez à niveau votre appareil mobile et perdez l'accès à l'application Microsoft Authenticator, ou si vous changez de numéro de téléphone et ne pouvez plus recevoir de SMS ou d'appels sur votre ancien numéro.

Avez-vous reçu l'invitation de vous inscrire de Metrolinx?

L'inscription à l'authentification multifactorielle se fait uniquement sur invitation. Vous auriez dû recevoir un courriel de Microsoft (invites@metrolinx.onmicrosoft.com) pour compléter l'inscription.

Si vous n'avez pas reçu l'invitation, veuillez attendre 24 heures avant de contacter le service de dépannage. Nous recommandons également de vérifier les dossiers des courriers indésirables dans votre boîte aux lettres. De plus, contactez le service de dépannage de votre organisation pour vous assurer que les courriels provenant de invites@metrolinx.onmicrosoft.com ne sont pas bloqués par votre système de courriel d'entreprise.

Vous ne pourrez pas vous inscrire à l'authentification multifactorielle sans le courriel d'invitation qui ressemble à l'image ci-dessous.

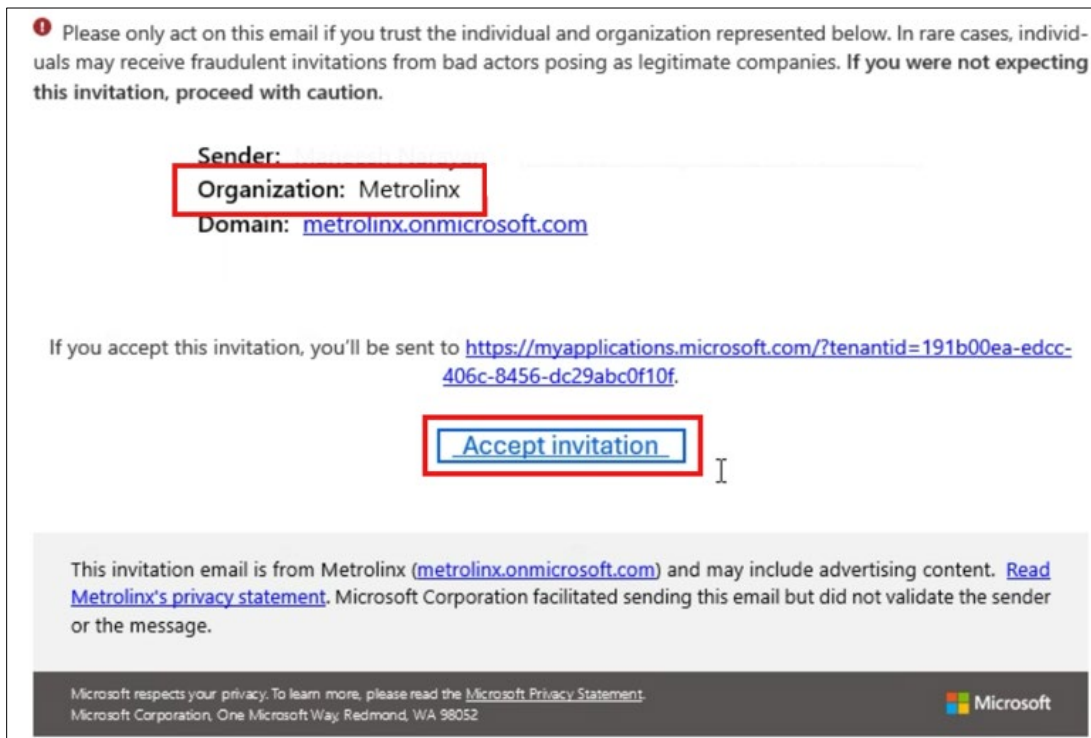


Avez-vous reçu votre invitation? Très bien. Commençons.

Accepter votre invitation à vous inscrire

Étape 1 : Accepter l'invitation pour commencer

Comme première étape, vous devez cliquer sur le lien « Accepter l'invitation » dans le courriel reçu.



Étape 2 : Vérifiez votre identité

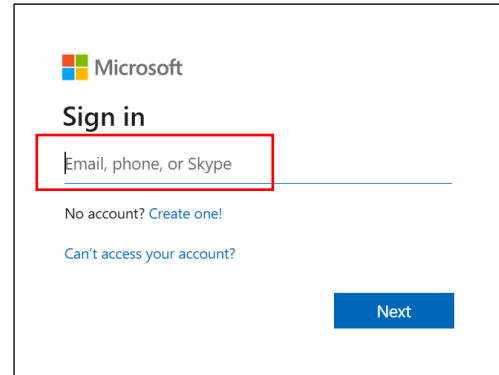
En cliquant sur « Accepter l'invitation », vous devrez vérifier votre identité. Selon votre adresse courriel, vous vous vérifierez avec l'une des trois méthodes suivantes.

Méthode 1 : Connectez-vous à votre compte d'organisation

Si votre adresse courriel existe déjà dans un locataire Microsoft Entra géré, vous vous authentifierez en vous connectant à votre compte d'organisation. Vous serez redirigé vers les pages de connexion de votre organisation pour vous authentifier en utilisant les informations d'identification de votre organisation.

Remarque importante : Si vous ne parvenez pas à vous connecter à votre compte d'organisation (par exemple, mot de passe oublié), veuillez contacter le service de dépannage de votre organisation pour obtenir de l'aide. Le service de dépannage de Metrolinx ne pourra pas vous aider à vous connecter à votre compte d'organisation.

Connectez-vous à votre compte d'organisation.



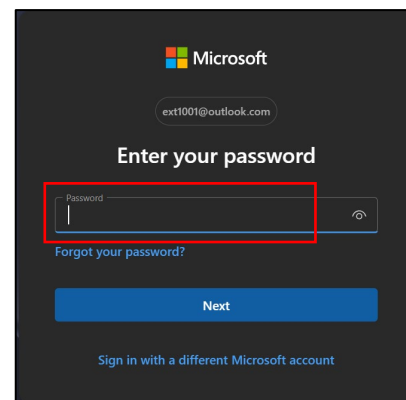
Remarque : À titre illustratif seulement. Les pages de connexion de votre organisation peuvent avoir un aspect différent avec le logo de votre organisation et l'image de marque.

Méthode 2 : Connectez-vous à votre compte Microsoft

Si votre adresse courriel est un compte Microsoft (par exemple, hotmail.com, outlook.com), vous vous authentifierez à votre compte en utilisant les identifiants de votre compte Microsoft personnel.

Remarque importante : Si vous ne parvenez pas à vous connecter à votre compte Microsoft (par exemple, mot de passe oublié), veuillez utiliser l'option de récupération de compte en libre-service pour récupérer votre compte. Le service de dépannage de Metrolinx ne pourra pas vous aider à vous connecter à votre compte Microsoft.

Connectez-vous à votre compte Microsoft.

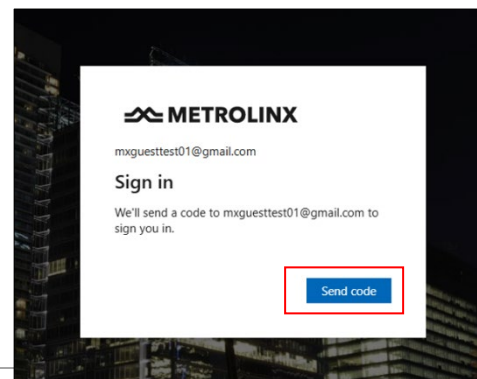


Méthode 3 : Connexion par un code d'accès envoyé par courriel

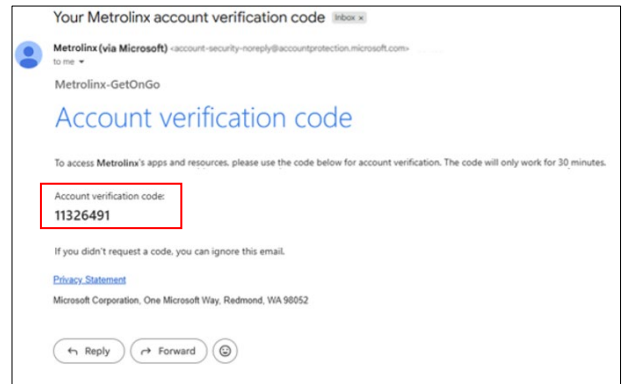
Si votre adresse courriel n'est ni un compte Microsoft Entra géré ni un compte Microsoft, un code d'accès vous sera envoyé par courriel pour vous vérifier.

Remarque importante : Si vous n'avez pas reçu le code d'accès par courriel, veuillez vérifier les dossiers des courriers indésirables dans votre boîte aux lettres avant de réessayer.

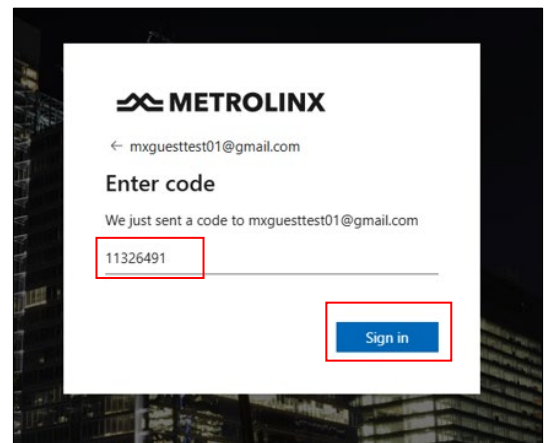
1. Cliquez sur le bouton « Envoyer le code » pour recevoir un code de courriel.



2. Obtenez le code d'accès de la boîte aux lettres.



3. Entrez le code d'accès de la boîte aux lettres et cliquez sur « Se connecter ».

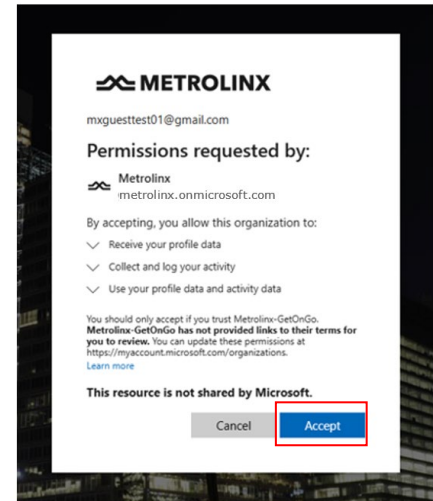


S'inscrire avec l'application Authenticator (Option A)

Étape 3 : S'inscrire à l'application Microsoft Authenticator (Option A)

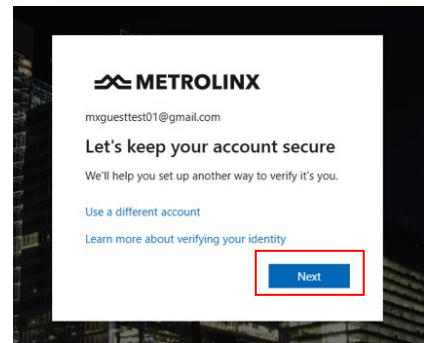
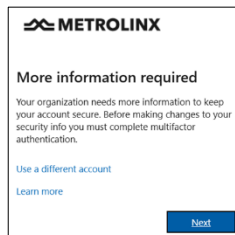
3.1 Accepter les autorisations

1. Acceptez la demande d'autorisations demandées pour vos données.

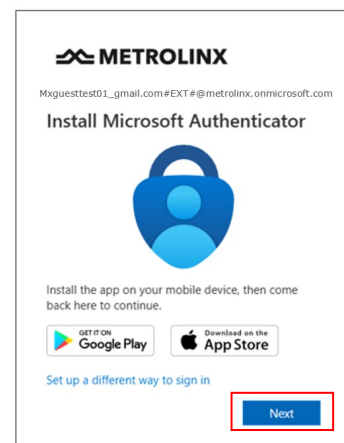


2. Cliquez sur « Suivant ».

Remarque : la capture d'écran incluse dans cette étape peut varier en fonction du domaine du compte que vous utilisez. Le titre peut indiquer « Plus d'informations requises ». Dans les deux cas, cliquez sur « Suivant ».



3. Cliquez sur « Suivant » pour continuer le téléchargement de l'application Microsoft Authenticator sur votre appareil mobile.



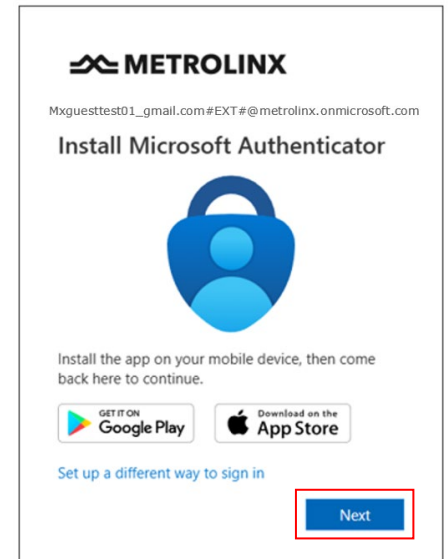
3.2 Téléchargez l'application Microsoft Authenticator (si elle n'est pas déjà installée)

Remarque : Si l'application Microsoft Authenticator est déjà installée sur votre appareil mobile, vous pouvez sauter les étapes 1 et 2. Cependant, veuillez vous assurer que l'application est mise à jour à la dernière version.

1. Ouvrez votre appareil mobile, accédez à la boutique d'applications et recherchez l'application « Microsoft Authenticator » OU balayez le code QR fourni à droite selon le type de votre appareil mobile.
2. Téléchargez l'application Microsoft Authenticator.

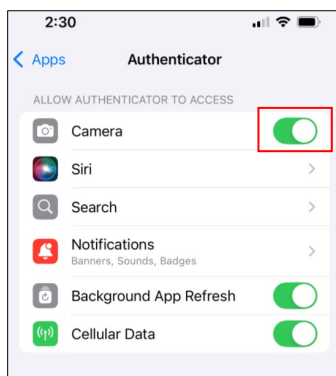
Remarque : À ce stade, si vous souhaitez vous inscrire pour le téléphone OTP comme méthode d'authentification multifactorielle au lieu de l'application Microsoft Authenticator, cliquez sur « **Configurer une autre façon de vous connecter** » et suivez les instructions dans la section « [Inscrivez-vous avec le téléphone \(Option B\)](#) ».

Important : lorsque vous ouvrez l'application Microsoft Authenticator, **veuillez accepter et autoriser l'application Microsoft Authenticator à vous envoyer des notifications et à accéder à votre caméra** (veuillez noter que cela ne signifie pas que l'application Microsoft Authenticator accède à vos photos). Il est nécessaire de compléter le processus d'inscription.

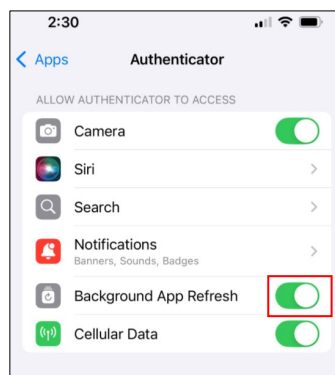


3. Si l'application n'a pas l'autorisation requise activée, allez dans l'application de paramètres de téléphone de votre appareil mobile, recherchez « Authenticator » et activez les autorisations suivantes :

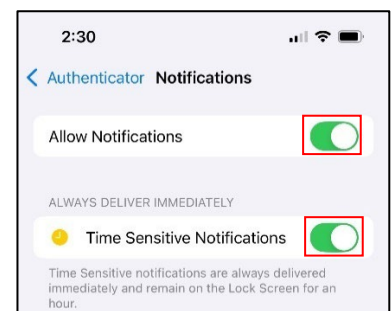
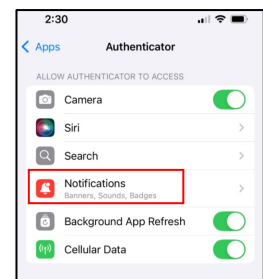
a) Autoriser l'accès à la caméra



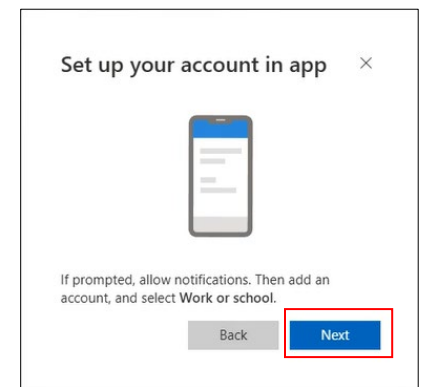
b) Activer la mise à jour de l'application en arrière-plan



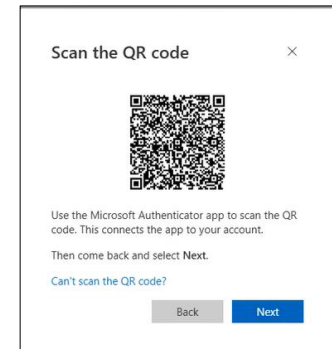
c) Autoriser les notifications



4. Une fois que vous avez téléchargé l'application Microsoft Authenticator avec les autorisations requises activées, cliquez sur « Suivant » pour confirmer que vous avez activé les notifications depuis votre appareil mobile.



5. Un écran de code QR s'affichera sur votre ordinateur pour ajouter votre compte dans l'application Authenticator, passez à la section suivante.

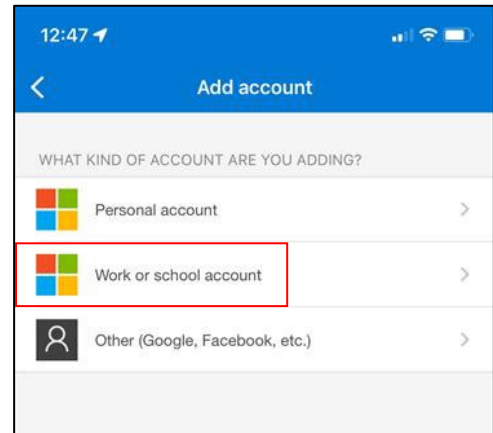


3.3 Ajoutez votre compte dans l'application Authenticator.

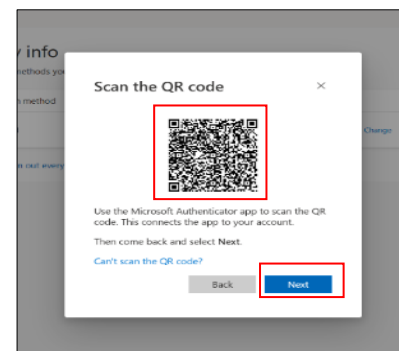
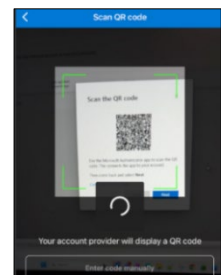
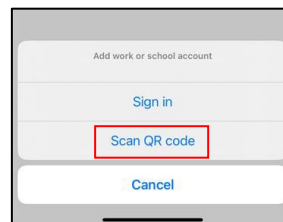
1. Sur votre appareil mobile, ouvrez l'application Microsoft Authenticator. Il se peut que des informations expliquant l'application vous soient présentées, sélectionnez « Ignorer ».
2. Cliquez sur « Ajouter un compte » (ou cliquez sur le + dans le coin droit si ce n'est pas la première fois que vous ajoutez un compte à l'application Microsoft Authenticator).
3. Si un message concernant une sauvegarde s'affiche*, sélectionnez « Continuer ».

**Lors de l'enregistrement d'un appareil Apple, vous pouvez recevoir un message vous demandant si vous souhaitez sauvegarder votre appareil sur iCloud (les utilisateurs Android ne recevront pas cette invite). Cela vous permettrait de restaurer votre inscription à l'authentification multifactorielle en cas de perte de votre appareil sans avoir à vous inscrire de nouveau. Notez que ni accepter ni refuser la sauvegarde de votre appareil n'aura d'impact sur votre inscription initiale à l'authentification multifactorielle.*

4. Sélectionnez « compte professionnel ou scolaire »
5. Si vous utilisez l'application Microsoft Authenticator pour la première fois, vous recevrez un message indiquant « Authenticator souhaite accéder à la caméra » (veuillez noter que cela ne signifie pas qu'Authenticator accède à vos photos), cliquez sur « Ok ».



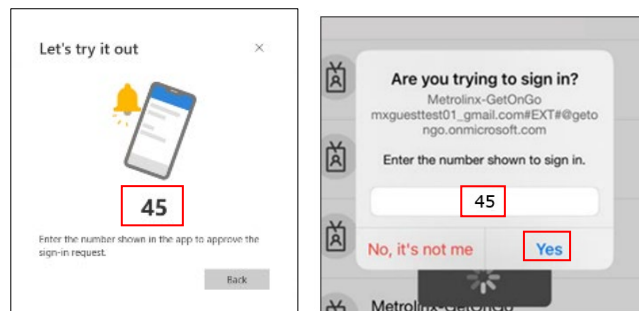
6. Cliquez sur « Balayez le code QR » et balayez le code QR affiché sur l'écran de votre ordinateur à l'aide de la caméra de votre appareil mobile. Cela ajoutera votre compte Metrolinx à votre application Microsoft Authenticator sur votre appareil mobile.
7. Sur l'écran de votre ordinateur, seulement après avoir balayé le code QR, cliquez sur « Suivant » et attendez que le système ait terminé de vérifier l'état d'activation.



3.4 Compléter le processus d'inscription à l'application Authenticator.

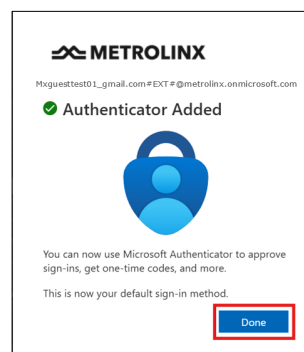
Une fois que votre compte est configuré sur votre appareil mobile, vous verrez un numéro affiché sur l'écran de votre ordinateur.

1. Entrez le numéro affiché sur l'écran de votre ordinateur dans votre appareil mobile et cliquez sur « Oui ».



2. Une fois terminé, un message de confirmation s'affichera sur l'écran de votre ordinateur pour confirmer que l'application Microsoft Authenticator a été ajoutée à votre compte.

3. Cliquez sur « Terminé ».



3.5 Remplir les conditions d'utilisation et la politique de confidentialité

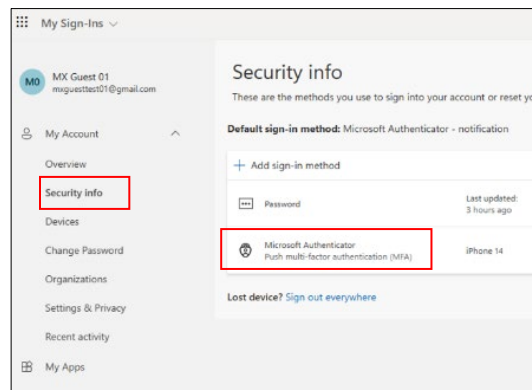
1. Lire les conditions d'utilisation de Metrolinx et le document de politique de confidentialité.
2. Cliquez sur « Accepter ».
3. Veuillez noter que l'acceptation est obligatoire. En cliquant sur « Accepter », vous serez redirigé vers la page <https://myapplications.microsoft.com>.



4. Pour confirmer l'inscription réussie, vérifiez que la méthode de connexion Microsoft Authenticator a été ajoutée dans la liste des méthodes de connexion pour votre compte en visitant la section « Informations de sécurité ».

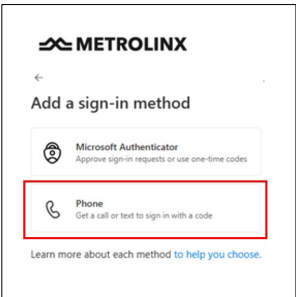
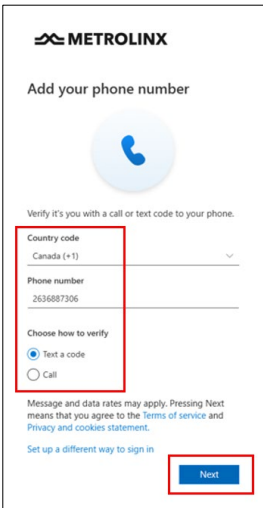
Remarque : Il se peut que vous soyez invité à vous authentifier à nouveau lors de la visite de la section « Informations de sécurité ».

Une fois vérifié, fermez la fenêtre du navigateur.

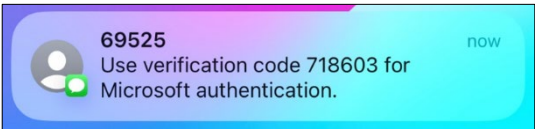
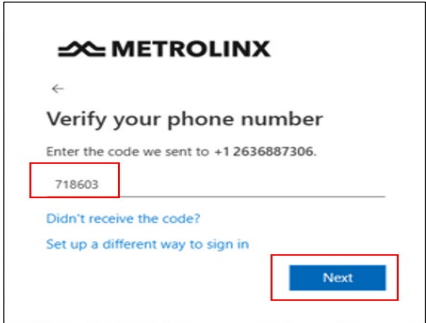


Inscrivez-vous par SMS ou téléphone (Option B)

a) Fournir un numéro de téléphone pour la vérification.

1. Cliquez sur « Téléphone » comme méthode d'authentification multifactorielle que vous souhaitez ajouter.	
2. Entrez le code de pays de votre numéro de téléphone 3. Entrez votre numéro de téléphone à utiliser comme méthode d'authentification multifactorielle 4. Sélectionnez la méthode de vérification : SMS ou appel téléphonique. 5. Cliquez sur « Suivant ». Le numéro de téléphone saisi doit être un numéro auquel vous avez accès et que vous pouvez utiliser pour vous authentifier.	

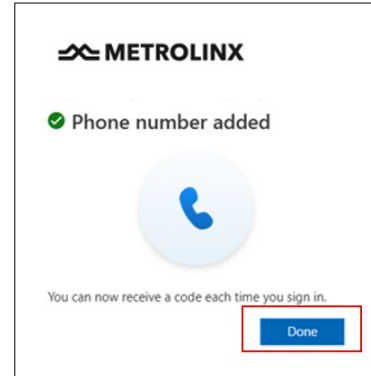
b) Confirmez votre compte par SMS.

1. Vous recevrez un code de vérification par SMS ou par appel téléphonique (selon la méthode sélectionnée à l'étape précédente) sur votre appareil mobile. <i>Il est important de ne pas masquer les alertes ni de bloquer l'expéditeur de ce code de vérification à l'avenir, car il sera utilisé pour recevoir les codes de vérification futurs en tant que méthode d'authentification multifactorielle. Si vous avez accidentellement masqué des alertes, affichez-les à nouveau dans la page de contact de ce contact. Si vous avez accidentellement bloqué l'expéditeur, retirez l'expéditeur de vos contacts bloqués dans les paramètres de votre téléphone.</i> 2. L'écran de votre ordinateur se mettra à jour pour vous demander de saisir le code de vérification reçu. Entrez le code de vérification reçu et cliquez sur « Suivant ».	 
--	---

Remarque : Si vous n'avez pas reçu le code, veuillez réessayer en utilisant l'option « Vous n'avez pas reçu le code? ».

L'écran affiché à droite sera affiché, indiquant que la vérification a réussi.

3. Cliquez sur « Terminé ».



4. Lire et « Accepter » les conditions d'utilisation.

Vous pouvez cliquer  pour ouvrir le document complet.

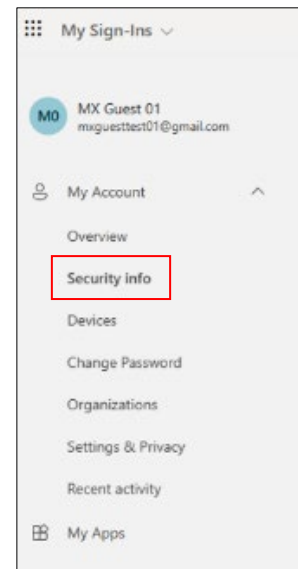


L'écran à droite sera affiché, ce qui signifie que vous vous êtes inscrit avec succès.

5. Vous pouvez fermer votre navigateur. Sinon, pour confirmer l'inscription réussie et vérifier que la méthode d'authentification Microsoft a été ajoutée dans la liste des méthodes de connexion pour votre compte en visitant la section « Informations de sécurité ».

Remarque : Il se peut que vous soyez invité à vous authentifier à nouveau lors de la visite de la section « Informations de sécurité ».

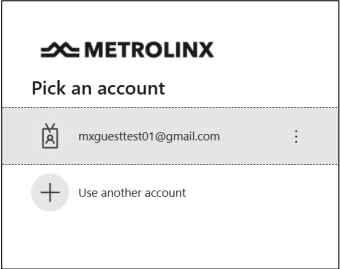
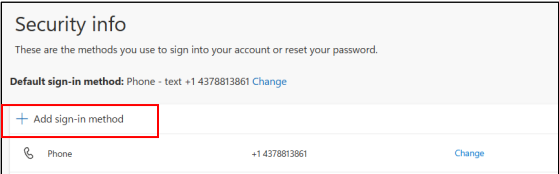
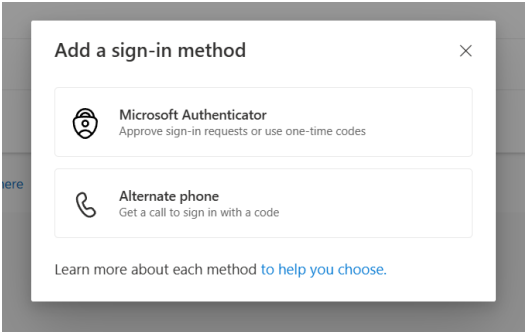
Une fois vérifié, fermez la fenêtre du navigateur.



Inscrire des méthodes supplémentaires pour l'authentification multifactorielle (facultatif)

Vous pouvez vous inscrire à **plusieurs méthodes d'authentification multifactorielle**. Cette section décrit le processus pour inscrire des méthodes supplémentaires après que vous vous soyez déjà inscrit avec au moins une méthode.

Connectez-vous à votre compte pour vous inscrire aux méthodes ou appareils supplémentaires.

1. Sur un ordinateur, ouvrez le lien suivant : https://aka.ms/mfasetup?tenant=191b00ea-edcc-406c-8456-dc29abc0f10f 2. Connectez-vous avec votre adresse courriel. 3. Une fois authentifié, vous arriverez sur la page d'information sur la sécurité.	
4. Cliquez sur « Ajouter une méthode de connexion » pour ajouter une nouvelle méthode d'authentification multifactorielle. 5. Sélectionnez votre méthode supplémentaire préférée et complétez son inscription, référez-vous aux étapes ci-dessus selon la méthode d'authentification multifactorielle (option A ou B) pour laquelle vous souhaitez vous inscrire pour votre compte. Si vous vous êtes déjà inscrit pour le téléphone (option B) comme méthode d'authentification multifactorielle, vous pouvez ajouter un numéro de téléphone supplémentaire en utilisant l'option « Ajouter un autre téléphone ». Si vous vous êtes déjà inscrit à l'application Authenticator (option A), vous pouvez également vous inscrire avec un deuxième appareil. Une fois que vous avez ajouté votre méthode d'authentification multifactorielle supplémentaire, fermez la fenêtre du navigateur.	 

FOIRE AUX QUESTIONS (FAQ) : Foire aux questions

QUESTIONS GÉNÉRALES

1. Qu'est-ce que l'authentification multifactorielle?

L'authentification multifactorielle est une fonction de sécurité qui aide à protéger les comptes en ligne en exigeant plus d'une forme de vérification avant d'accorder l'accès. Traditionnellement, vous aviez seulement besoin d'un mot de passe pour vous connecter, mais les mots de passe peuvent être volés ou devinés. L'authentification multifactorielle ajoute des couches de protection supplémentaires, telles qu'un code envoyé à votre téléphone, un code généré par une application d'authentification, ou une invitation dans une application d'authentification.

En utilisant l'authentification multifactorielle, vos comptes sont beaucoup moins susceptibles d'être compromis. L'authentification multifactorielle est maintenant une pratique courante et recommandée pour les organisations du monde entier afin de garder les données sûres et sécurisées. Elle est facile à configurer et à utiliser, et c'est l'un des moyens les plus efficaces de protéger les services en ligne et les données.

2. Comment l'authentification multifactorielle est-elle déployée chez Metrolinx?

Metrolinx déploie l'authentification multifactorielle pour renforcer la sécurité des applications en ligne et protéger les informations sensibles. Le processus de déploiement est conçu pour être simple et convivial, garantissant que tous les utilisateurs peuvent facilement s'inscrire et utiliser l'authentification multifactorielle. Le déploiement se fait en étapes, en commençant par un projet pilote composé d'un groupe sélectionné d'utilisateurs et d'employés de la TI à partir de décembre 2025. Cela sera suivi d'un déploiement à tous les utilisateurs internes et externes restants en janvier 2026. Les ressources de soutien – y compris les guides étape par étape, les FAQ et l'aide au service de dépannage – seront disponibles pour aider tout le monde tout au long du processus.

Metrolinx utilise Microsoft Entra ID (anciennement Azure Active Directory) comme plateforme principale pour l'authentification multifactorielle. Les utilisateurs devront enregistrer un appareil mobile ou télécharger une application d'authentification (Microsoft Authenticator). Une fois inscrit, vous serez invité à vérifier votre identité avec un code ou un avis d'approbation lors de l'accès aux applications protégées, en particulier depuis de nouveaux appareils ou emplacements.

Les équipes IT et helpdesk de Metrolinx surveilleront de près le déploiement, prêtes à aider en cas de problème technique. Cette approche par phases aidera à minimiser les perturbations et à garantir que tout le monde bénéficie du soutien dont il a besoin. L'objectif est de rendre l'adoption de l'authentification multifactorielle aussi fluide que possible tout en améliorant considérablement la sécurité de l'environnement numérique de Metrolinx.

3. Quels sont les avantages de l'authentification multifactorielle?

L'authentification multifactorielle offre plusieurs avantages importants tant pour les personnes que pour les organisations comme Metrolinx. L'avantage principal est une sécurité considérablement améliorée. En exigeant deux formes de vérification ou plus – l'authentification multifactorielle rend beaucoup plus difficile pour les cybercriminels d'obtenir un accès non autorisé à vos comptes.

Un autre avantage important est la protection des données sensibles. Avec l'authentification multifactorielle en place, les informations confidentielles, les dossiers financiers et les données personnelles sont beaucoup moins susceptibles d'être exposés en cas d'attaque d'hameçonnage ou d'atteinte à la protection des données. Cela aide Metrolinx à maintenir la conformité avec les règlements en matière de protection de la vie privée et à instaurer la confiance avec les employés et les partenaires.

L'authentification multifactorielle réduit également le risque de vol d'identité et de fraude. Cette approche par couches de la sécurité est particulièrement importante pour les organisations qui dépendent des services basés sur le nuage et de l'accès à distance.

4. En m'inscrivant à l'authentification multifactorielle, Metrolinx pourra-t-il suivre mon appareil ou voir mon activité?

L'authentification multifactorielle ne permet pas à Metrolinx de voir quoi que ce soit sur votre appareil mobile, de suivre votre emplacement ou l'activité de votre appareil. Vos renseignements personnels sont protégés.

5. Quelles applications sont activées et appliquées avec Microsoft Entra ID?

À compter du 31 mars 2026, l'accès aux applications suivantes nécessitera l'authentification multifactorielle – iSupplier, Oracle Primavera Unifier et Oracle Aconex.

6. Dans quelles situations suis-je tenu de m'authentifier par l'authentification multifactorielle?

L'authentification multifactorielle sera requise chaque fois que vous accédez à une application protégée, sauf si vous avez une session active existante d'un identifiant précédent.

7. Ai-je besoin d'être connecté à Internet pour utiliser Microsoft Authenticator?

Oui. Pour recevoir des notifications poussées de connexion et envoyer votre réponse, votre appareil doit être connecté à Internet.

QUESTIONS RELATIVES À L'INSCRIPTION

1. Qui est tenu de s'inscrire à l'authentification multifactorielle?

Tous les partenaires de Metrolinx qui doivent s'inscrire recevront un courriel (deinvitation@metrolinx.onmicrosoft.com) pour s'inscrire et enregistrer l'authentification multifactorielle. Si vous recevez un tel courriel, veuillez vous inscrire dès que possible.

2. Comment puis-je m'inscrire?

Veuillez suivre les étapes décrites dans ce document.

3. Que se passe-t-il si je ne m'inscris pas à l'authentification multifactorielle?

À partir du 31 mars 2026, Metrolinx commencera progressivement à appliquer l'appel d'offres pour les demandes d'entreprise. Si une tentative d'accès nécessite l'authentification multifactorielle et que vous ne vous êtes pas encore inscrit, vous serez obligé de vous inscrire à l'authentification multifactorielle avant de pouvoir accéder à l'application. Nous vous recommandons fortement de vous inscrire dès que possible.

4. J'ai des problèmes pour accéder au lien d'invitation pour commencer le processus d'inscription. À qui puis-je parler?

Veuillez appeler le service de dépannage au 416-202-5000 (option n° 3 dans l'annuaire) pour obtenir de l'aide.

5. Puis-je utiliser une autre application mobile, non Microsoft, telle que Google Authenticator?

Non, seule l'application d'authentification Microsoft est prise en charge.

6. L'application Microsoft Authenticator peut-elle être installée sur un ordinateur?

Non, elle ne peut pas être installée sur un ordinateur. L'application doit être installée sur un iPhone ou un appareil Android.

7. Puis-je utiliser un numéro de téléphone au lieu d'utiliser l'application Microsoft Authenticator sur l'appareil mobile?

Vous pouvez utiliser un numéro de téléphone au lieu de l'application Microsoft Authenticator. Cependant, utiliser l'application Microsoft Authenticator est la méthode facile, plus sécurisée et recommandée pour s'inscrire à l'authentification multifactorielle.

8. Ai-je besoin d'un appareil mobile pour installer l'application Microsoft Authenticator?

Oui, vous aurez besoin d'un appareil mobile (c.-à-d. iPhone ou Android) pour installer Microsoft Authenticator.

9. Puis-je avoir plusieurs appareils avec Microsoft Authenticator installé?

Oui, vous pouvez installer Microsoft Authenticator sur plusieurs appareils (par exemple, un appareil mobile de l'entreprise ou un appareil personnel).

10. Si j'ai deux appareils avec Microsoft Authenticator installé, les notifications arriveront-elles sur les deux appareils?

Oui, si vous avez plus d'un appareil avec Microsoft Authenticator installé, les deux appareils recevront une invitation de notification lorsque vous devrez compléter l'authentification multifactorielle. Vous ne serez tenu d'utiliser qu'un des appareils pour approuver la notification.

11. Je n'ai pas reçu d'appareil mobile de la part de mon employeur. Comment puis-je m'inscrire?

L'utilisation d'un appareil mobile personnel pour l'inscription à l'authentification multifactorielle est prise en charge.

12. J'ai un nouveau téléphone avec le même numéro, et je n'avais auparavant enregistré que Microsoft Authenticator. Je ne peux plus utiliser Microsoft Authenticator.

Veuillez appeler le service de dépannage au 416-202-5000 (option n° 3 dans l'annuaire) pour obtenir de l'aide.

13. J'ai un nouveau téléphone avec le même numéro. J'ai précédemment enregistré mon appareil pour Microsoft Authenticator ainsi que mon numéro de téléphone. Je ne peux plus utiliser Microsoft Authenticator.

Authentifiez-vous sur [Entra ID](#) et suivez les instructions dans ce document pour installer et enregistrer Microsoft Authenticator sur votre nouveau téléphone pour l'authentification multifactorielle.

14. Mon téléphone a été réinitialisé ou nettoyé. Je ne peux plus utiliser Microsoft Authenticator pour me connecter. Je n'ai pas enregistré mon numéro de téléphone comme méthode d'authentification de rechange.

Veuillez appeler le service de dépannage au 416-202-5000 (option n° 3 dans l'annuaire) pour obtenir de l'aide.

15. Mon téléphone a été réinitialisé ou nettoyé. Je ne peux pas utiliser Microsoft Authenticator pour me connecter. J'ai un numéro de téléphone enregistré avant que mon téléphone ne soit réinitialisé ou nettoyé.

Authentifiez-vous sur [Entra ID](#) et suivez les instructions de ce document pour installer et enregistrer Microsoft Authenticator sur votre nouveau téléphone pour l'authentification multifactorielle.

16. J'ai perdu mon appareil configuré à l'authentification multifactorielle – Comment dois-je procéder?

Veuillez appeler le service de dépannage au 416-202-5000 (option n° 3 de l'annuaire) immédiatement pour signaler la perte de l'appareil d'authentification multifactorielle et obtenir une aide supplémentaire.