

Guide sur l'authentification multifactorielle

Accéder aux ressources de Metrolinx avec
l'authentification unique et l'authentification
multifactorielle de Microsoft Entra ID

Guide de l'utilisateur externe et FAQ

Content

Objectifs et conditions préalables.....	1
Votre expérience de connexion pour les applications protégées par authentification multifactorielle d'Entra ID.....	2
Vos scénarios de connexion : Comment accédez-vous aux ressources de Metrolinx?	2
Étape 1 : Accédez à votre application et vérifiez votre identité.....	3
Étape 2 : S'inscrire à l'authentification multifactorielle.....	4
Étape 2A : Enregistrement avec l'application Authenticator (Option A)	5
Étape 2B : S'inscrire avec SMS ou téléphone (Option B)	10
Étape 3 : Connexion avec l'authentification multifactorielle	12
Connexion réussie.....	16
Enregistrer des méthodes d'authentification multifactorielle supplémentaires (facultatif).....	17
FOIRE AUX QUESTIONS : Foire aux questions.....	19
QUESTIONS GÉNÉRALES	19
QUESTIONS D'INSCRIPTION À L'AUTHENTIFICATION MULTIFACTORIELLE	20
QUESTIONS DE CONNEXION RELATIVE À L'AUTHENTIFICATION MULTIFACTORIELLE.....	21

Objectifs et conditions préalables

Ce guide vous guide à travers le processus de connexion pour les utilisateurs ayant un **compte non Metrolinx** aux ressources de Metrolinx protégées par Microsoft Entra ID avec authentification multifactorielle.

Une liste des applications de Metrolinx protégées par Microsoft Entra ID :

- Microsoft Office 365 (Teams, SharePoint, Outlook, Word, Excel, Power BI, etc.)
- Oracle Primavera Unifier
- Oracle Aconex
- Oracle iSupplier

Pour toutes les autres applications non énumérées ci-dessus, vous continuerez à vous authentifier avec Okta.

Si vous rencontrez des problèmes avec Entra ID, vous pouvez contacter le service de dépannage par téléphone au **416-202-5000** (option du répertoire n° 3).

Pour tout problème spécifique à l'application, vous pouvez contacter l'équipe de soutien de la demande respective chez Metrolinx.

Votre expérience de connexion pour les applications protégées par authentification multifactorielle d'Entra ID

Metrolinx migre graduellement ses applications vers Microsoft Entra ID. À mesure que cette migration progresse, vous remarquerez des changements dans la façon dont vous vous connectez aux applications suivantes. Cependant, la manière dont vous accédez à vos applications ne changera pas.

Veuillez consulter le tableau ci-dessous pour les applications concernées et les changements de connexion spécifiques.

Applications	Changements à la connexion
Applications Microsoft Office 365 (Teams, SharePoint, Word, Excel, PowerPoint, Outlook, Power BI, etc.)	Transfert d'Okta à Microsoft Entra ID avec l'authentification multifactorielle pour l'accès aux applications. Vous ne serez plus invité à vous authentifier en utilisant la page de connexion d'Okta.
Oracle Aconex Construction Engineering Ouverture de session sur Aconex	Transfert de l'authentification native à Microsoft Entra ID avec l'authentification multifactorielle. Après avoir fourni votre nom de connexion ou votre courriel de travail sur la page d'ouverture de session d'Aconex, vous serez automatiquement redirigé vers la page de connexion Microsoft pour vous connecter.
Oracle Primavera P6 et Unifier	Transfert de l'authentification gérée par Oracle à Microsoft Entra ID avec l'authentification unique et l'authentification multifactorielle. Vous vous connecterez directement par la page de connexion Microsoft.
Oracle iSupplier	

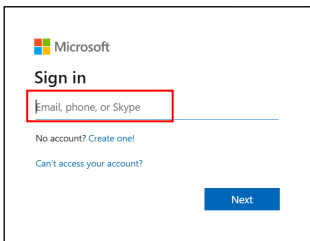
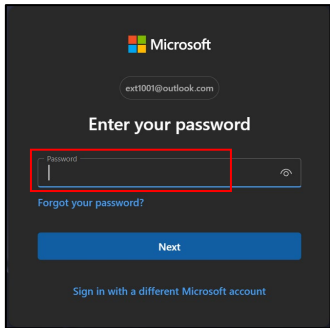
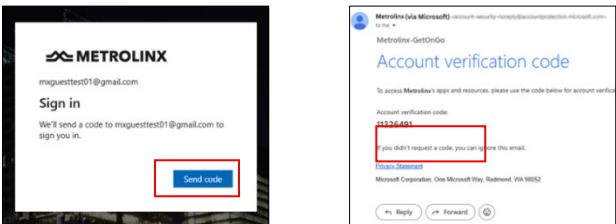
Vos scénarios de connexion : Comment accédez-vous aux ressources de Metrolinx?

Vos étapes de connexion varieront en fonction de la manière dont vous accédez aux ressources de Metrolinx. Le fait de ne pas avoir enregistré votre compte pour l'authentification multifactorielle aura un impact sur votre processus de connexion.

Scénario de connexion	Étapes de connexion
Mon compte n'a pas été enregistré pour l'authentification multifactorielle	1. Naviguez vers l'application comme vous le faites habituellement, ou utilisez le lien fourni dans le tableau de l'application ci-dessus. 2. Vérifiez votre identité (Étape 1). 3. Complétez le processus d'inscription à l'authentification multifactorielle (étape 2) lors de la connexion pour un accès continu aux applications protégées par Entra ID. Une fois terminé, vous serez automatiquement redirigé et connecté à votre demande.
Mon compte est déjà enregistré pour l'authentification multifactorielle	1. Naviguez vers l'application comme vous le faites habituellement, ou utilisez le lien fourni dans le tableau de l'application ci-dessus. 2. Vérifiez votre identité (Étape 1). 3. Connectez-vous avec l'authentification multifactorielle (Étape 3) à votre demande en utilisant la ou les méthodes enregistrées de votre compte.

Pour éviter tout problème lié à la connexion une fois les modifications appliquées, vous devrez peut-être redémarrer votre appareil.

Étape 1 : Accédez à votre application et vérifiez votre identité

1. Naviguez vers votre application souhaitée comme vous le feriez normalement, ou utilisez le Tableau d'application de l'expérience de connexion pour un lien direct vers votre application.	 Naviguer vers votre application
2. Lorsque vous accédez aux applications protégées d'Entra ID, vous devrez vérifier votre identité en utilisant l'une des trois méthodes ci-dessous en fonction de votre adresse courriel.	
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. <i>Remarque importante :</i> 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.	 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. <i>Remarque importante :</i> 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.	
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.	

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. Récupérez et saisissez le code d'accès depuis la boîte aux lettres, **puis cliquez sur « Se connecter »**.



Étape 2 : S'inscrire à l'authentification multifactorielle

L'authentification multifactorielle est un processus d'authentification qui ajoute une couche supplémentaire de sécurité lors de l'accès à vos applications ou systèmes en vous demandant à la fois votre nom d'utilisateur et mot de passe et un **second facteur** (application Microsoft Authenticator ou numéro de téléphone) pour valider votre identité.

Le tableau ci-dessous résume les options du deuxième facteur que vous pouvez utiliser.

Option	Renseignements	Recommandé à...
2A 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
2B 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.

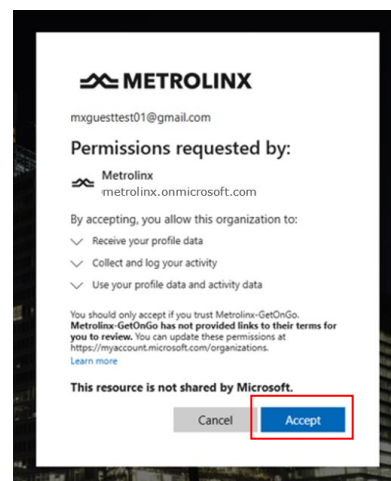
Nous recommandons d'enregistrer les deux options d'authentification multifactorielle afin de prévenir les interruptions de connexion futures et de minimiser le besoin d'aide au service d'assistance dans les cas où une méthode spécifique d'authentification multifactorielle n'est pas disponible. Par exemple, 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.

Étape 2A : Enregistrement avec l'application Authenticator (Option A)

Étape 2A.1 : Accepter la demande d'autorisations

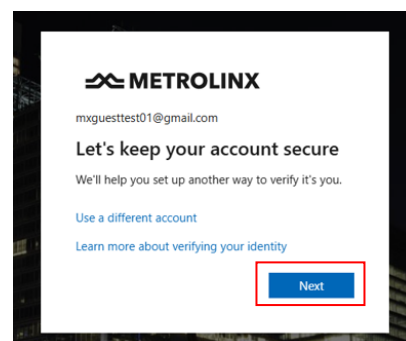
1. Après avoir vérifié votre identité, il se peut que l'on vous demande **d'accepter** l'invite pour les autorisations demandées par Metrolinx.

Si vous avez déjà accepté la demande d'autorisations, alors cette étape serait sautée.



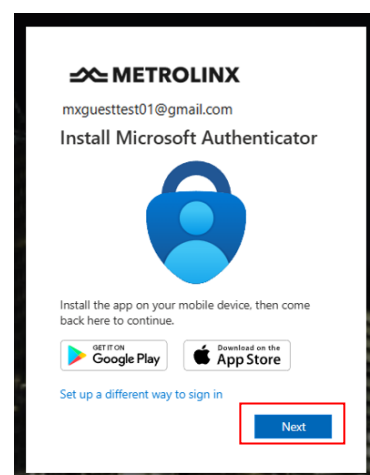
2. Cliquez sur « **Suivant** » pour commencer le processus d'inscription.

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.

Si vous souhaitez vous inscrire par appel vocal par téléphone comme méthode d'authentification multifactorielle au lieu de l'application Microsoft Authenticator, cliquez sur « **Configurer une autre méthode de connexion** » et suivez les instructions de [la section 2B : S'inscrire avec SMS ou téléphone \(Option B\)](#).

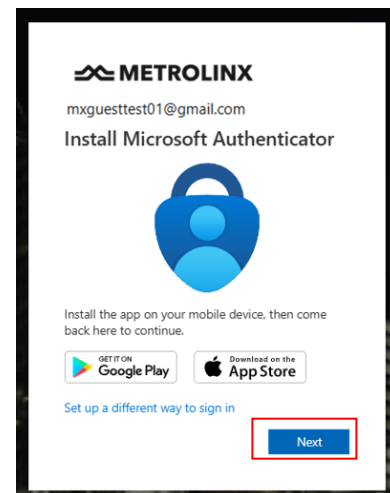


Étape 2A.2 : Téléchargez l'application Microsoft Authenticator (si elle n'est pas déjà installée)

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.

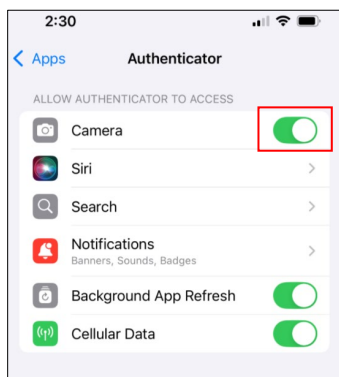
Important : lorsque vous ouvrez l'application Microsoft Authenticator, veuillez accepter et autoriser l'application Microsoft Authenticator à vous envoyer des notifications et à accéder à votre caméra (veuillez noter que cela ne signifie pas que l'application Microsoft Authenticator accède à vos photos).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



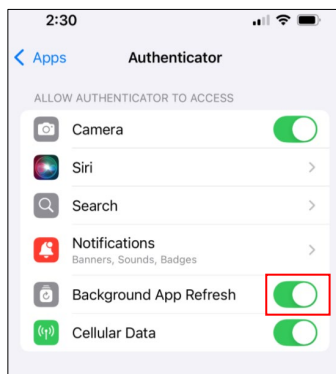
3. Si l'application n'a pas l'autorisation requise activée, allez dans l'application de paramètres de téléphone de votre appareil mobile, recherchez « Authenticator » et activez les autorisations suivantes :

**Les étapes ci-dessous varieront selon les différents modèles d'appareils mobiles et versions.*

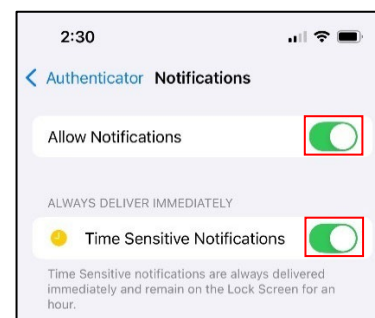
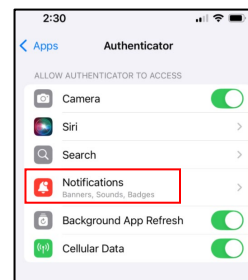
a) Autoriser l'accès à la caméra



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

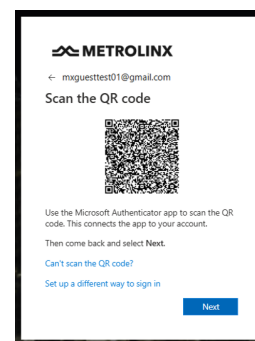
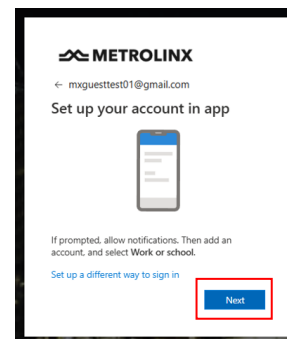


c) Autoriser les notifications



- 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.

- Un écran de code QR s'affichera sur votre ordinateur pour ajouter votre compte dans l'application Authenticator, passez à la section suivante. **Ne cliquez pas sur « Suivant », car vous devrez balayer le code QR avec votre appareil mobile.**

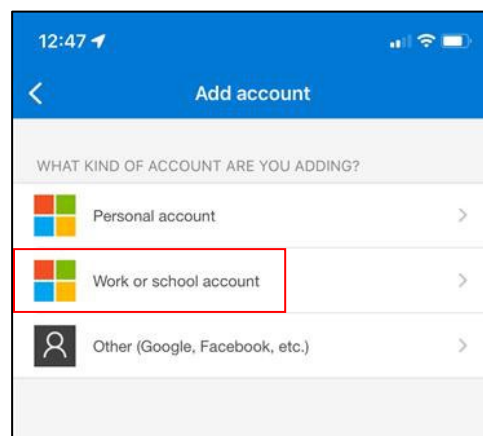


Étape 2A.3 : Ajoutez votre compte dans l'application Authenticator

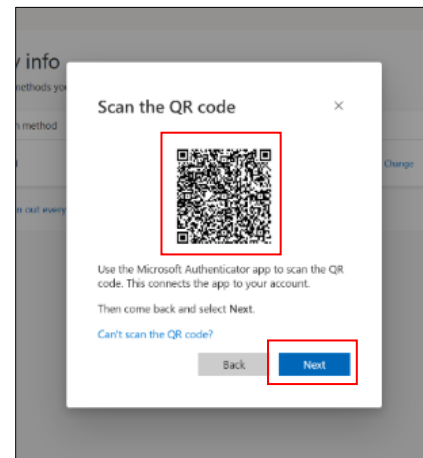
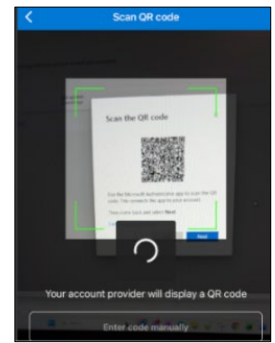
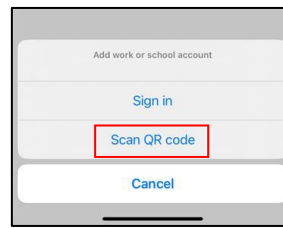
- Sur votre appareil mobile, ouvrez l'application Microsoft Authenticator. Il se peut que des informations expliquant l'application vous soient présentées, sélectionnez « **Ignorer** ».
- Cliquez sur « **Ajouter un compte** » (ou cliquez sur le + dans le coin droit si ce n'est pas la première fois que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

- Sélectionnez « **compte professionnel ou scolaire** »
- Si vous utilisez l'application 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** ».



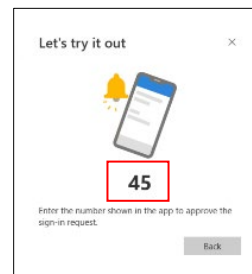
6. Cliquez sur « **Balayez le code QR** » et **balayez le code QR** affiché sur l'écran de votre ordinateur à l'aide de la caméra de votre appareil mobile. Cela ajoutera votre compte Metrolinx à votre application Microsoft Authenticator sur votre appareil mobile.
7. Sur l'écran de votre ordinateur, seulement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



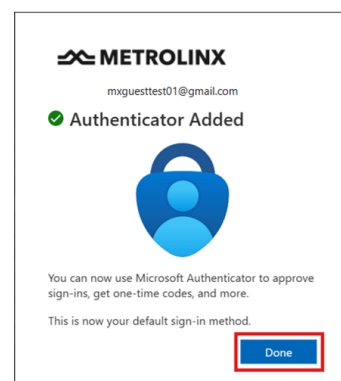
Étape 2A.4 : Compléter le processus d'inscription de l'application Authenticator

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

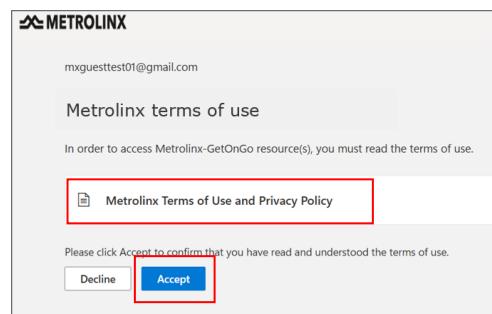
1. Entrez le numéro affiché sur l'écran de votre ordinateur dans votre appareil mobile et cliquez sur « **Oui** ».



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** ».



4. Acceptez les conditions d'utilisation et la politique de confidentialité en **cliquant** sur la case du document pour lire et « **Accepter** ».



Après une inscription réussie, vous recevrez un accès à votre demande. Pour une capture d'écran montrant à quoi ressemble une connexion réussie à chaque application, consultez la section [Connexion Réussie](#).

Pour tout problème d'authentification dans votre application par Entra ID, consultez la section [FAQ](#).

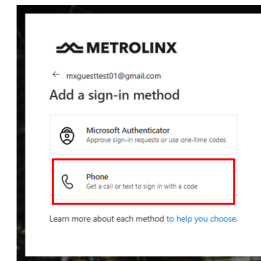


Connexion réussie avec l'authentification multifactorielle

Étape 2B : S'inscrire avec SMS ou téléphone (Option B)

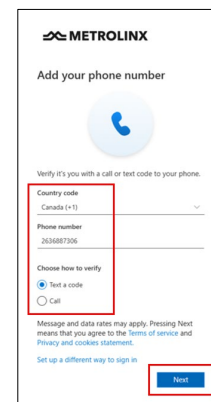
Étape 2B.1 : Fournissez votre numéro de téléphone

1. Cliquez sur « **Téléphone** » comme méthode d'authentification multifactorielle que vous souhaitez ajouter.



2. Entrez votre **code de pays de téléphone** et votre numéro de téléphone à utiliser comme méthode d'authentification multifactorielle
3. **Sélectionnez** la méthode de vérification : SMS ou appel téléphonique.
4. Cliquez sur « **Suivant** ».

Le numéro de téléphone saisi doit être un numéro auquel vous avez accès et que vous pouvez utiliser pour vous authentifier.



Étape 2B.2 : Compléter le processus d'inscription par téléphone

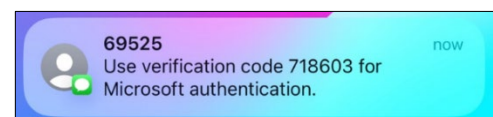
5. Vous recevrez un code de vérification par SMS ou par appel téléphonique (selon la méthode sélectionnée à l'étape précédente) sur votre appareil mobile.

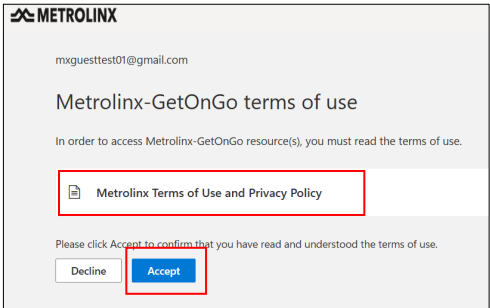
Il est important de ne pas masquer les alertes ni de bloquer l'expéditeur de ce code de vérification à l'avenir, car il sera utilisé pour recevoir les codes de vérification futurs en tant que méthode d'authentification multifactorielle.

- 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.

6. 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? ».



<i>L'écran affiché à droite sera affiché, indiquant que la vérification a réussi.</i> 7. Cliquez sur « Terminé ».	
8. Acceptez les conditions d'utilisation et la politique de confidentialité en cliquant sur la case du document pour lire et « Accepter ».	
Après une inscription réussie, vous recevrez un accès à votre demande. Pour une capture d'écran montrant à quoi ressemble une connexion réussie à chaque application, consultez la section Connexion Réussie. Pour tout problème d'authentification dans votre application par Entra ID, consultez la section FAQ.	Connexion réussie avec l'authentification multifactorielle

Étape 3 : Connexion avec l'authentification multifactorielle

L'authentification multifactorielle est un processus d'authentification qui ajoute une couche supplémentaire de sécurité lors de l'accès à vos applications ou systèmes. Après avoir saisi votre nom d'utilisateur et votre mot de passe, il vous sera demandé de vérifier votre identité en utilisant un **deuxième facteur déjà enregistré sur votre compte**, comme **l'application Microsoft Authenticator** ou un code envoyé à votre **appareil mobile** par appel téléphonique ou SMS.

Au lieu de vous fier uniquement à votre mot de passe, l'authentification multifactorielle aide à protéger votre compte en exigeant cette étape de vérification supplémentaire à chaque connexion.

1. Après [avoir vérifié votre identité](#), complétez l'authentification multifactorielle en utilisant l'un des deuxièmes facteurs que vous auriez déjà enregistrés à votre compte :
 - Pour utiliser [l'application Authenticator](#), consultez la **méthode 1**.
 - Pour utiliser le code de vérification par [appel téléphonique](#), consultez la **méthode 2**.
 - Pour utiliser le code de vérification par [SMS](#), consultez la **méthode 3**.

**Les étapes décrites dans chaque méthode varieront selon les différents modèles d'appareils mobiles et versions.*

Pour la **méthode 1**, en utilisant l'application Microsoft Authenticator :

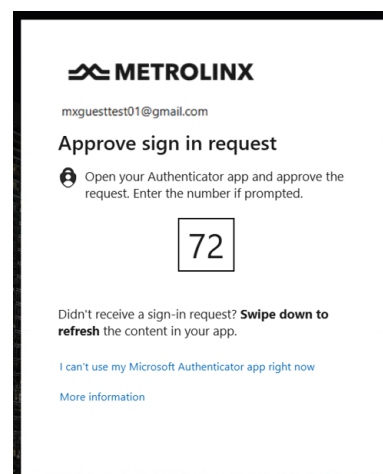
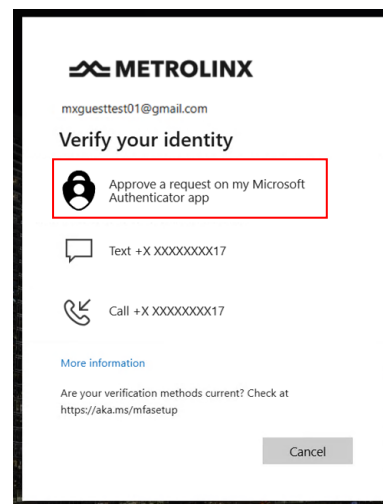
Assurez-vous que votre appareil mobile est connecté à Internet.

Cliquez sur l'option Authenticator pour vérifier votre identité.

Pour approuver votre demande de connexion, un numéro sera affiché sur votre écran, que vous devez saisir dans votre application d'authentification (une notification peut être déclenchée sur votre téléphone pour faciliter l'utilisation).



Une fois terminée, votre demande d'inscription sera approuvée et vous aurez complété votre authentification.



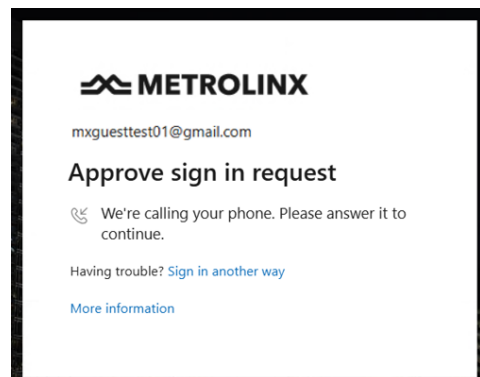
Pour la **méthode 2**, utilisation du code de vérification par appel téléphonique :

Cliquez sur l'option « Appeler +X XXXXXXXX17 », le numéro de téléphone enregistré sur le compte que vous utilisez pour vous connecter.



Répondez à l'appel téléphonique et suivez ses instructions pour approuver votre demande de connexion.

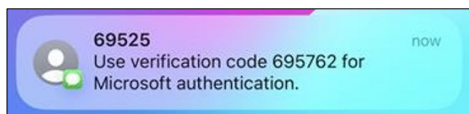
Une fois terminée, votre demande d'inscription sera approuvée et vous aurez complété votre authentification.



Pour la **méthode 3**, utilisation du code de vérification par SMS :

Cliquez sur l'option « Texter +X XXXXXXXX17 » correspondant au numéro de téléphone enregistré sur le compte que vous utilisez pour vous connecter.

Vous recevrez un code de vérification sur votre téléphone mobile.



Entrez le code de vérification envoyé à votre appareil mobile sur la page de connexion d'Entra ID et cliquez sur « Vérifier » pour vous authentifier.



Après une authentification réussie, vous recevrez un accès à votre demande. Pour une capture d'écran montrant à quoi ressemble une connexion réussie à chaque application, consultez la section [Connexion réussie](#).

Pour tout problème, consultez la section [FAQ](#).



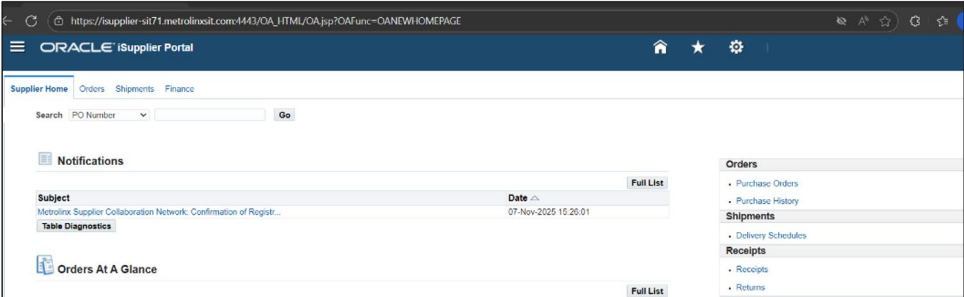
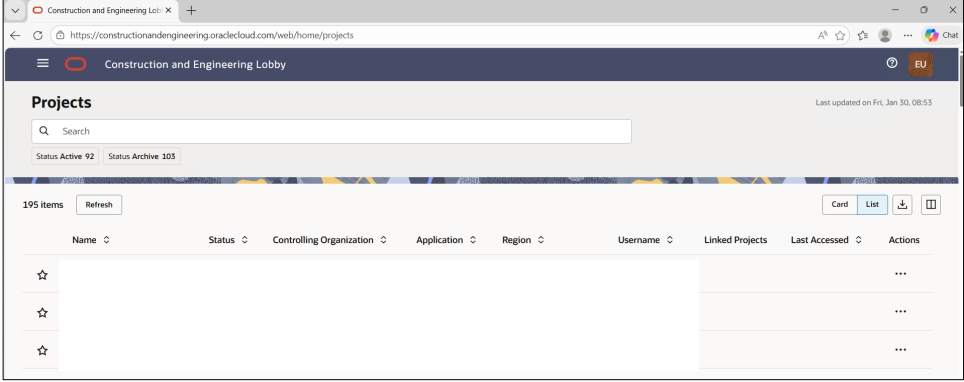
Connexion réussie avec l'authentification multifactorielle

*Si vous n'êtes pas en mesure de compléter **l'une** des nombreuses méthodes de vérification que l'on vous demande de réaliser, vous pouvez gérer vos méthodes d'authentification multifactorielle enregistrées à partir de la page [Informations de sécurité](#) dans votre profil Entra ID.*

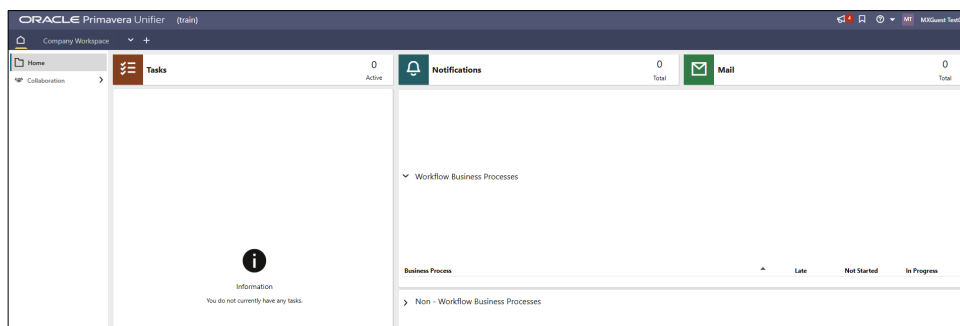
*Si vous êtes incapable de compléter **l'une** des méthodes de vérification requises, contactez le service de dépannage de Metrolinx pour obtenir de l'aide par téléphone au : 416-202-5000 (option directe n° 3).*

Connexion réussie

Cette section affiche l’achèvement d’une connexion à authentification unique ou à authentification multifactorielle réussie des applications protégées de Microsoft Entra ID. **Bien que le processus de connexion ait changé, les applications ne l’ont pas fait.**

Applications Microsoft Office 365 (Teams, Word, Excel, PowerPoint, Outlook, Power BI, etc.)	
Oracle iSupplier	
Oracle Aconex <i>*Pour vous connecter, vous devrez d’abord fournir votre nom de connexion ou votre courriel de travail sur la page de connexion Oracle Aconex avant de vous authentifier avec Microsoft Entra ID.</i>	
Oracle Primavera P6	

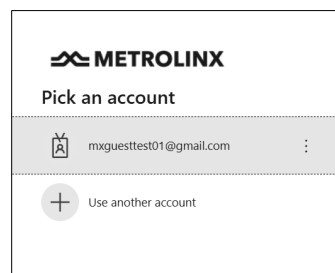
Oracle Primavera Unifier



Enregistrer des méthodes d'authentification multifactorielle supplémentaires (facultatif)

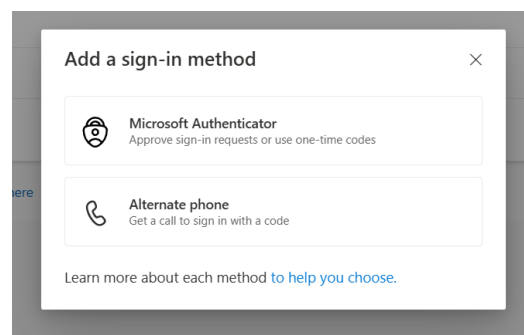
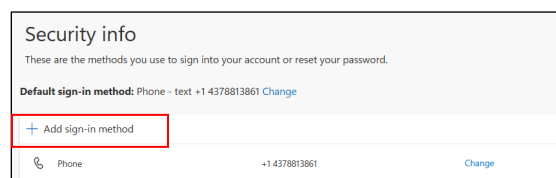
Vous pouvez enregistrer plusieurs méthodes d'authentification multifactorielle. Cette section décrit le processus pour enregistrer des méthodes supplémentaires que vous pouvez utiliser, après avoir déjà enregistré avec succès une méthode.

1. Sur un ordinateur, ouvrez la page [Informations de sécurité](#) de votre profil Microsoft Entra ID de Metrolinx.
2. Connectez-vous avec l'adresse courriel que vous utilisez pour accéder aux ressources de Metrolinx.
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 inscrit auparavant pour le téléphone (option B) comme méthode d'authentification multifactorielle, vous pouvez **ajouter un numéro de téléphone supplémentaire** en utilisant l'option « Ajouter un téléphone de rechange ».



- Si vous vous êtes déjà inscrit à l'application Authenticator (option A), vous pouvez **enregistrer un deuxième appareil mobile.**

Une fois que vous avez ajouté votre méthode d'authentification multifactorielle supplémentaire, fermez la fenêtre du navigateur.

FOIRE AUX QUESTIONS : Foire aux questions

QUESTIONS GÉNÉRALES

1. Qu'est-ce que Microsoft Entra ID?

Microsoft Entra ID est le dernier service de gestion de l'identité et des accès basé sur le nuage de Metrolinx. Il est conçu pour aider Metrolinx à gérer et contrôler de manière sécurisée l'accès à nos ressources et applications d'entreprise en utilisant l'authentification unique et l'authentification multifactorielle.

2. 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.

3. Pourquoi ai-je besoin de l'authentification multifactorielle?

En accord avec notre engagement continu envers la cybersécurité et la confiance du public, Metrolinx migre ses applications et ressources vers Microsoft Entra ID en tant que principal fournisseur d'identité. En conséquence, les applications Microsoft Office 365 (Teams, Outlook, Word et autres) ainsi que certaines applications Oracle passeront à l'utilisation de Microsoft Entra ID. Cependant, l'accès à toutes les autres applications non répertoriées dans ce document continuera d'utiliser la même méthode d'authentification qu'actuellement jusqu'à nouvel avis.

4. Devrai-je continuer à utiliser Okta?

Oui, vous continuerez à utiliser Okta pour accéder à toutes les autres applications qui n'ont pas encore migré vers Entra ID. Toutes les applications non listées dans ce document continueront d'utiliser la même méthode d'authentification qu'elles utilisent actuellement jusqu'à nouvel avis.

5. Et si je n'avais pas enregistré mon compte pour l'authentification multifactorielle?

Si vous n'avez pas enregistré votre compte pour l'authentification multifactorielle, vous serez obligé d'enregistrer votre compte lorsque vous tenterez d'accéder à l'une des applications protégées de Microsoft Entra ID une fois qu'elles auront été migrées vers Entra ID.

QUESTIONS D'INSCRIPTION À L'AUTHENTIFICATION MULTIFACTORIELLE

1. 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.

2. Puis-je utiliser d'autres applications mobiles autres que Microsoft, telles que Google Authenticator?

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

3. 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.

1. 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.

2. 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.

3. 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).

4. 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 DE CONNEXION RELATIVE À L'AUTHENTIFICATION MULTIFACTORIELLE

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

Une authentification multifactorielle sera requise chaque jour où vous accédez à une application protégée par Microsoft Entra ID.

2. Pourquoi me demande-t-on d'enregistrer une méthode d'authentification multifactorielle lors de la connexion à une demande?

En accord avec notre engagement continu envers la cybersécurité et la confiance du public, Metrolinx migre ses applications et ressources vers Microsoft Entra ID en tant que principal fournisseur d'identité. En conséquence, les applications Microsoft Office 365 (Teams, Outlook, Word et autres) ainsi que certaines applications Oracle passeront à l'utilisation de Microsoft Entra ID. Cependant, l'accès à toutes les autres applications non répertoriées dans ce document continuera d'utiliser la même méthode d'authentification qu'actuellement jusqu'à nouvel avis. Pour les instructions sur la façon de compléter votre inscription à l'authentification multifactorielle, veuillez vous référer à la section [Inscription à l'authentification multifactorielle](#) de ce document.

3. Pourquoi ai-je des difficultés à accéder à mon application?

Il y a plusieurs raisons. Si l'on vous demande de « Sécuriser votre compte » en vous inscrivant à l'AMF, veuillez alors compléter le processus d'inscription décrit dans la section [Inscription](#) à l'AMF de ce document.

Pour tout autre problème après avoir terminé l'inscription, contactez le service de dépannage par téléphone au 416-202-5000 (option de l'annuaire n° 3)

4. Puis-je changer le deuxième facteur de vérification (téléphone ou application d'authentification) que l'on me demande de compléter lors de la connexion à une application?

Oui, vous pouvez changer la méthode de deuxième facteur par défaut dans le portail Microsoft Entra ID à partir de la page [Informations de sécurité](#). Cependant, vous ne pouvez choisir que parmi les méthodes déjà enregistrées dans votre compte. Pour les instructions, consultez le *Guide de modification des paramètres d'authentification multifactorielle*.

Pour enregistrer des méthodes d'authentification supplémentaires sur votre compte, vous pouvez également utiliser la page [Informations de sécurité](#) et vous référer à la section [Enregistrer des méthodes d'authentification multifactorielle supplémentaires](#) de ce document.

5. Que faire si je n'ai plus accès à mon deuxième facteur (téléphone ou application Authenticator)?

Si vous avez plusieurs facteurs, tels qu'un téléphone ou une application d'Authenticator, enregistrés sur votre compte et que vous pouvez toujours utiliser, alors vous pouvez modifier vos méthodes dans le portail Microsoft Entra ID à partir de la page [Informations de sécurité](#). Pour les instructions, consultez le *Guide de modification des paramètres d'authentification multifactorielle*.