

Multifactor Authentication (MFA) with Microsoft Entra ID

Enrollment Process using an IOS mobile device

External User Guide & FAQ

December 2025

Content

Objectives and prerequisites	2
Participating in the MFA Enrollment Rollout.....	2
Multifactor Authentication (MFA) for mobile options	3
Have you received the invite to register from Metrolinx?.....	4
Accept Your Invitation to Register	5
Enroll with Authenticator App (Option A).....	8
Enroll with SMS or phone (Option B)	13
Enroll additional MFA methods (Optional)	15
FAQ: Frequently Asked Questions	16
GENERAL QUESTIONS	16
ENROLLMENT QUESTIONS	18

Objectives and prerequisites

This guide takes you through the Multifactor Authentication enrollment process for users who access Metrolinx resources using a **non-Metrolinx account**, including the three options available (see table summarizing options on page 2).

To complete this process, you will need to have:

- An IOS mobile device
 - If you are using an Android mobile device, refer to the MFA Enrollment Guide for Android devices.
- an invitation email from Metrolinx to sign-up for MFA from invites@Microsoft.ca
 - If you have not received an email invitation, check your Junk and SPAM folders before contacting Help Desk.

Should you experience any difficulties in enrolling for MFA, you can contact the Help Desk for support at: 416-202-5000 (directory option 3)

Participating in the MFA Enrollment Rollout

As of December 2025, Metrolinx has begun rolling out Single Sign-On (SSO) & Multi-Factor Authentication (MFA) using Microsoft Entra ID for access to the following Oracle applications as of March 30, 2026: iSupplier, Oracle Primavera Unifier, and Oracle Aconex.

If you are participating in this rollout, you will have received an email from SSO_MFA_EntraID@Metrolinx.com on **January 20, 2026**, with reference to this Guide for how to register your account for Multifactor Authentication (MFA) at Metrolinx.

Please follow the instructions below to complete your account registration and help better secure Metrolinx digital assets.

Multifactor Authentication (MFA) for mobile options

During the enrollment process you will be asked to select an MFA option. The table below summarizes your options. Once you have decided on which option to enroll in, please proceed to the appropriate section on page 5.

Option	Details	Recommended to...
A Microsoft Authenticator	***Recommended option*** - Requires a smart mobile device with iOS 16.0 or later* - Requires downloading the Microsoft Authenticator app	- Users who have a smart mobile device - Users who want to enroll multiple devices
B Phone (SMS or Voice OTP)	- Does not require a smart mobile device* (compatible with older mobile devices) - Requires connection to a mobile network (i.e., will NOT work in Airplane Mode)	Users who do not have a smart mobile device*

**A smart mobile device has internet access and can download applications.*

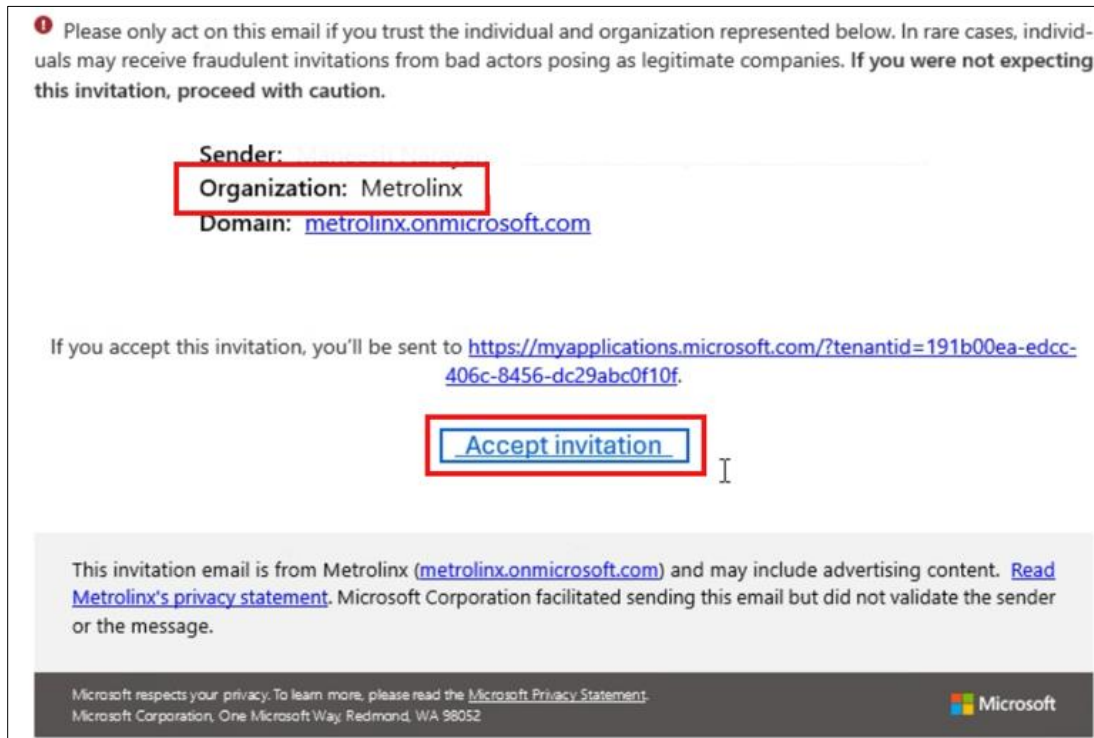
We recommend registering both MFA options to prevent future login interruptions and minimize the need for helpdesk assistance in cases where a specific MFA method is unavailable. For example, if you upgrade your mobile device and lose access to the Microsoft Authenticator app, or if you change your phone number and can no longer receive SMS or calls on your old number.

Have you received the invite to register from Metrolinx?

MFA enrollment is by invitation only. You should have received an email from Microsoft (invites@microsoft.com) to complete sign-up.

If you have not received the invitation, please wait 24 hours before contacting the Help Desk. We also recommend checking SPAM and Junk folders in your mailbox. Additionally, contact your organization's IT department to ensure emails from invites@microsoft.com are not being blocked by your corporate email system.

You will not be able to enroll for MFA without the invitation email which looks like the image below.

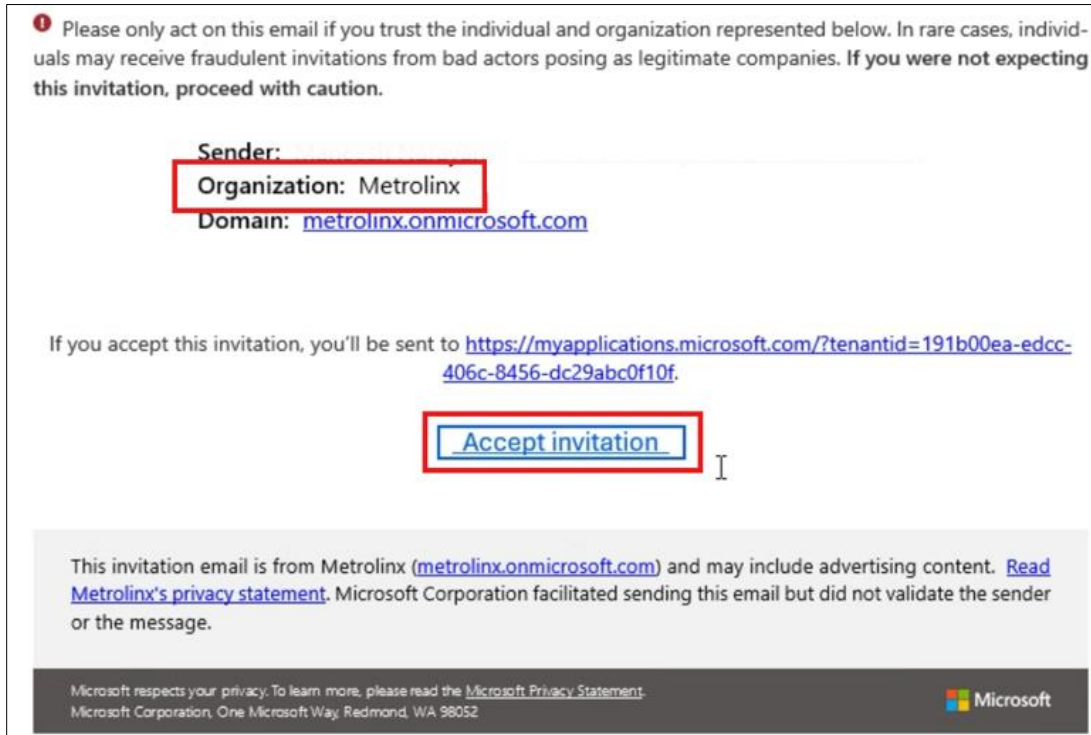


Received your invite? Great! Let's get started.

Accept Your Invitation to Register

Step 1: Accept the invitation to get started

As the very first step, you are required to click the "Accept Invitation" link in the email received.



Step 2: Verify your identity

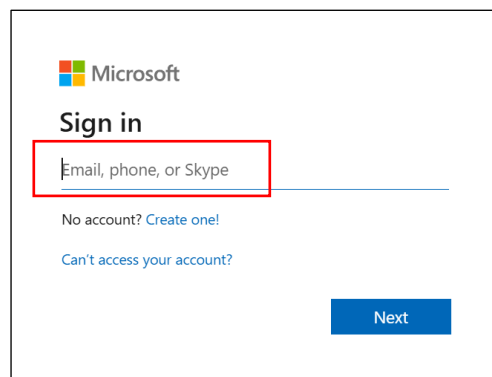
On clicking “Accept Invitation”, you will be required to verify your identity. Depending on your email address, you will verify yourself with one of the following three methods.

Method 1: Login to your organization account

If your email address already exists in a managed Microsoft Entra tenant, you will verify yourself by logging in to your organization account. You will be redirected to your organization’s login pages to authenticate using your organization credentials.

Important Note: If you are unable to login to your organization account (e.g., forgot password), please contact your organization’s IT helpdesk for assistance. Metrolinx IT helpdesk will not be able to assist you in logging in to your organization account.

Login to your organization account.



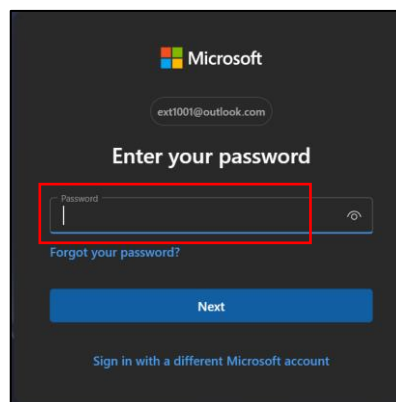
Note: For illustration purposes only. Your organization’s login pages may look different with your organization logo and branding.

Method 2: Login to your Microsoft Account

If your email address is a Microsoft Account (e.g., hotmail.com, outlook.com), you will authenticate to your account using personal Microsoft account credentials.

Important Note: If you are unable to login to your Microsoft account (e.g., forgot password), please use self-service account recovery option to recover your account. Metrolinx IT helpdesk will not be able to assist you in logging in to your Microsoft account.

Login to your Microsoft account.

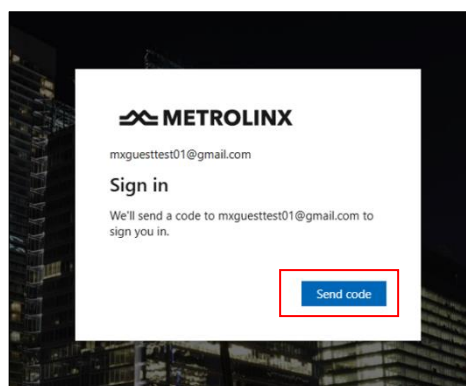


Method 3: Login through email-based passcode

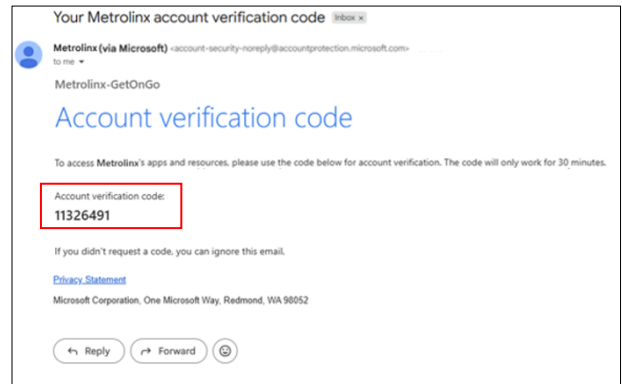
If your email address is neither a managed Microsoft Entra tenant account nor a Microsoft Account, you will be sent a passcode to your email to verify yourself.

Important Note: If you have not received the email passcode, please check the SPAM or Junk folders in your mailbox before trying again.

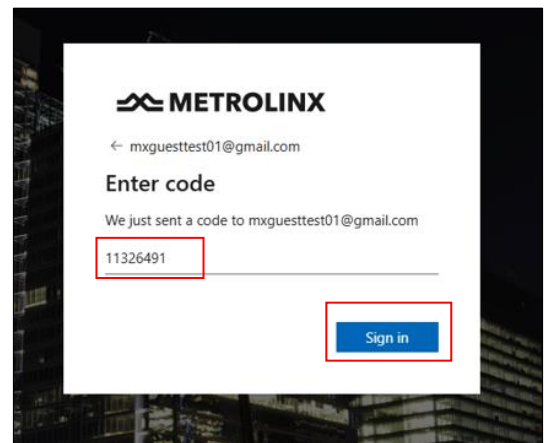
1. Click “Send Code” button to receive an email passcode.



2. Get the passcode from the mailbox.



3. Enter the passcode from the mailbox and click "Sign-in".

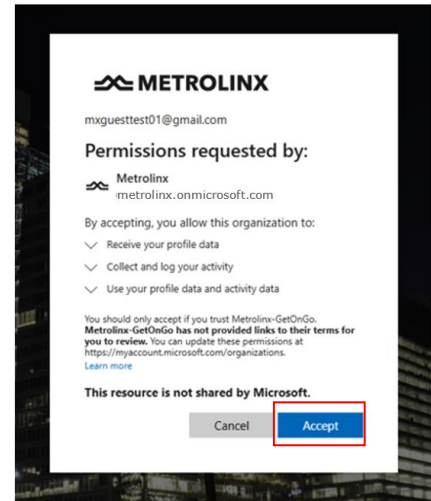


Enroll with Authenticator App (Option A)

Step 3: Enroll for Microsoft Authenticator app (Option A)

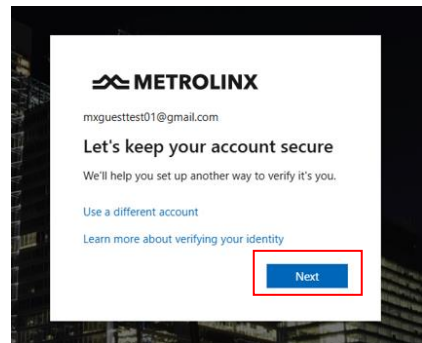
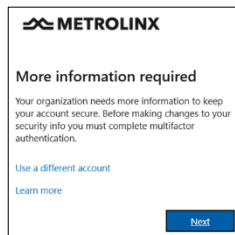
3.1 Accept permissions

1. Accept the prompt for **permissions requested** to your data.

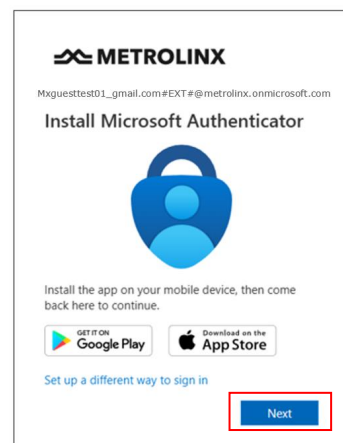


2. Click "Next".

Note: the screenshot included in this step may vary depending on the account domain you are using. The title may read "More information required". In both cases, click "Next".



3. Click "Next" to proceed downloading the Microsoft Authenticator application on your mobile device.



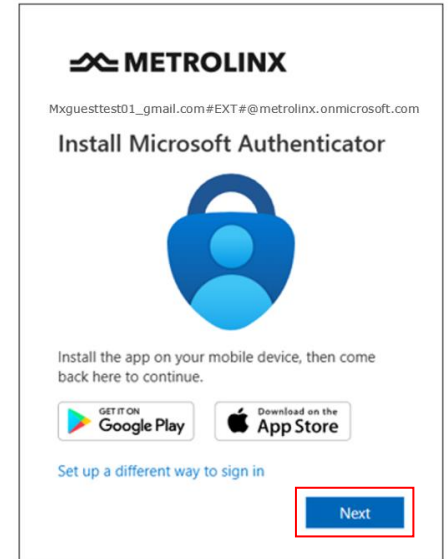
3.2 Download the Microsoft Authenticator app (if not already installed)

Note: If the Microsoft Authenticator application is already installed on your mobile device, you can skip steps 1 and 2.

1. Open your mobile device, access the application store and search for the "Microsoft Authenticator" app OR scan the QR code provided on the right according to your mobile device type.
2. Download the Microsoft Authenticator app.

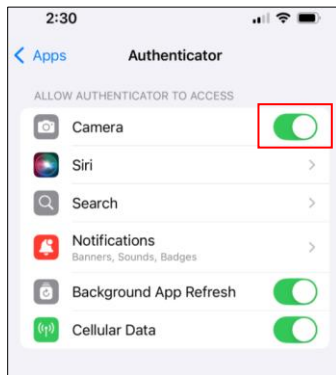
Note: At this point, if you want to enroll for Phone OTP as MFA method instead of Microsoft Authenticator app, click '**Set up a different way to sign in**' and follow the instructions in section "[Enroll with Phone \(Option B\)](#)".

Important: when you open the Microsoft Authenticator app, **please accept and allow the Microsoft Authenticator app to send you notifications and access your camera** (please note that it does not mean that the Microsoft Authenticator app is accessing your photos). It is required to complete the enrollment process.

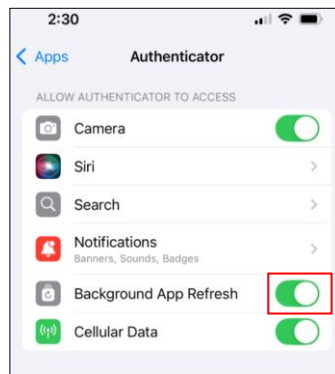


3. If the application does not have the required permission enabled, go to your mobile device phone settings app, search for "Authenticator" and enable the following permissions:

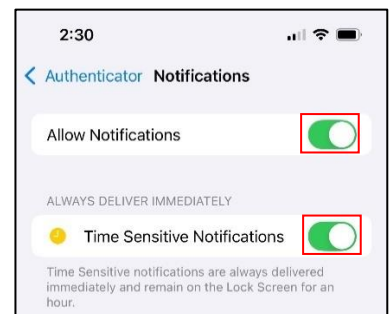
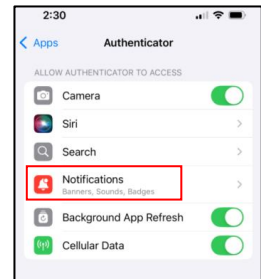
a) Allow access to camera



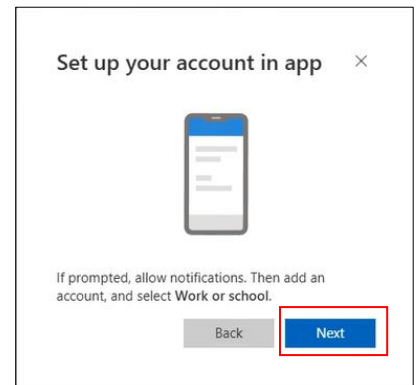
b) Enable Background App Refresh



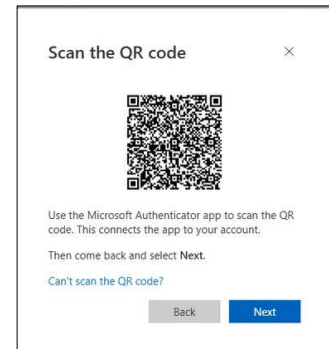
c) Allow notifications



4. Once you have the Microsoft Authenticator app downloaded with the required permissions enabled, click "Next" to confirm you have enabled notifications from your mobile device.



5. A QR code screen will be displayed on your computer to add your account in the Authenticator application, proceed to the next section.

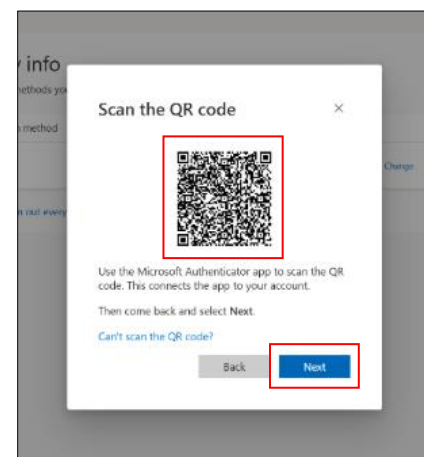
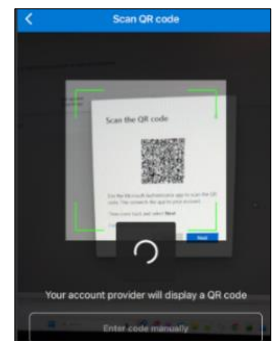
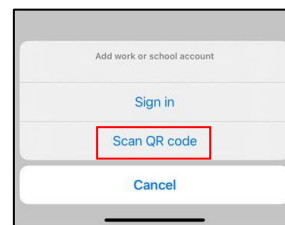
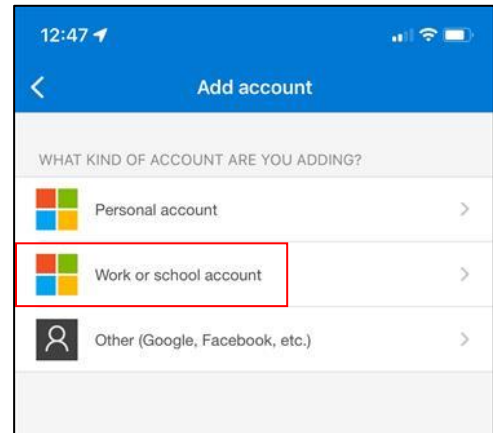


3.3 Add your account in the Authenticator application.

1. On your mobile device, open the Microsoft Authenticator application. You may be presented information explaining the app, select "Skip".
2. Click "Add an account" (or click on the + in the right-hand corner if it is not the first time that you add an account to Microsoft Authenticator app).
3. If a message about a backup is displayed*, select "Continue".

**When registering an Apple device, you may receive a message asking if you would like to back-up your device to the iCloud (Android users will not receive a prompt). This would allow you to restore your MFA registration in the event you lose your device without having to enroll a subsequent time. Note that neither accepting nor declining to back-up your device will impact your initial MFA enrollment.*

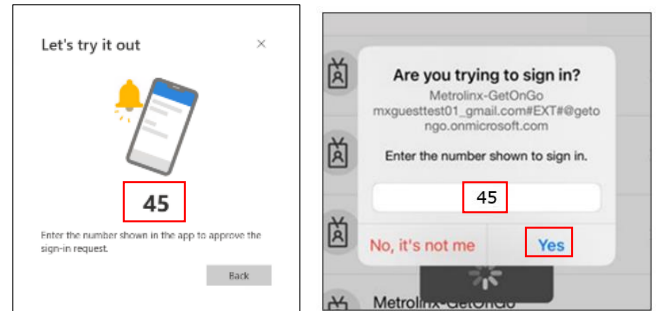
4. Select "Work or school account"
5. If you are using the Microsoft Authenticator app for the first time, you will receive a prompt saying "Authenticator would like to access the camera" (please note that it does not mean that Authenticator is accessing your photos), click "Ok".
6. Click "Scan QR Code" and scan the QR code displayed on your computer screen using the mobile device camera. This will add your Metrolinx account to your Microsoft Authenticator application on your mobile device.
7. On your computer screen, only after you have scanned the QR code, click "Next" and wait until the system has finished checking the activation status.



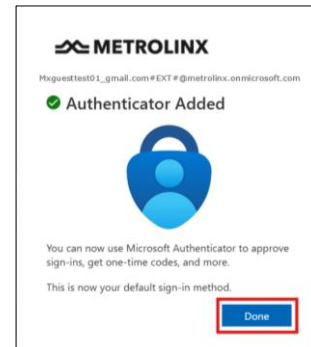
3.4 Complete the Authenticator app enrollment process.

Once your account is set up on your mobile device, you will see a number displayed on your computer screen.

1. Enter the number displayed on your computer screen in your mobile device and click "Yes".



2. Once completed, a confirmation message will be displayed on your computer screen to confirm that Microsoft Authenticator application has been added to your account.
3. Click "Done".



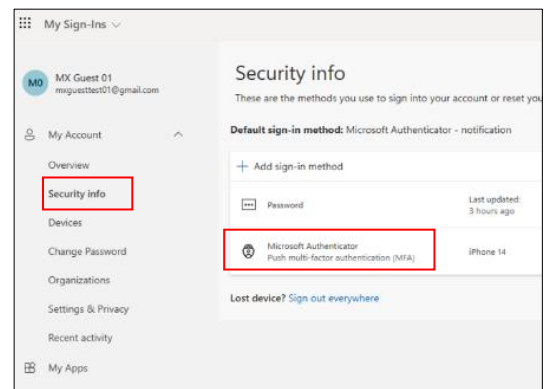
3.5 Complete the Terms of Use and Privacy Policy

1. Read Metrolinx Terms of Use and Privacy Policy Document.
2. Click "Accept".
3. Please note acceptance is mandatory. On clicking "Accept", you will be redirected to the <https://myapplications.microsoft.com> page.



4. To confirm successful enrollment, validate that the Microsoft Authenticator sign-in method was added in the list of sign-in methods for your account by visiting the "Security Info" section.

Note: You may be asked to authenticate again when visiting the "Security Info" section.



Enroll with SMS or phone (Option B)

a) Provide phone number for verification.

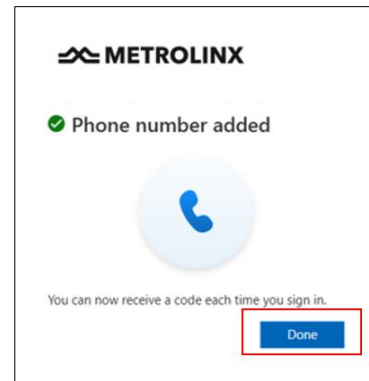
1. Click "Phone" as your MFA method you would like to add.	
2. Enter your phone number country code 3. Enter your phone number to be used as MFA method 4. Select verification method: SMS or Phone call. 5. Click "Next". The phone number entered should be a number you have access to and can use to authenticate yourself with.	

b) Confirm your account by SMS.

1. You will receive a verification code by SMS or by phone call (according to the method selected in the previous step) on your mobile device. <i>It is important to not hide alerts of or block the sender of this verification code in the future as it will be used to received future verification codes as MFA method. If you have accidentally hidden alerts, unhide alerts in the contact page of this contact. If you have accidentally blocked the sender, remove the sender from your blocked contacts in your phone settings.</i> 2. Your computer screen will update asking you to input the verification code received. Enter the verification code received and click "Next". Note: If you did not receive the code, please try again using the option "Didn't receive the code?".	
--	--

The screen shown on the right will be displayed, indicating that the verification was successful.

3. Click "Done".



4. Read and "Accept" Terms of Use.

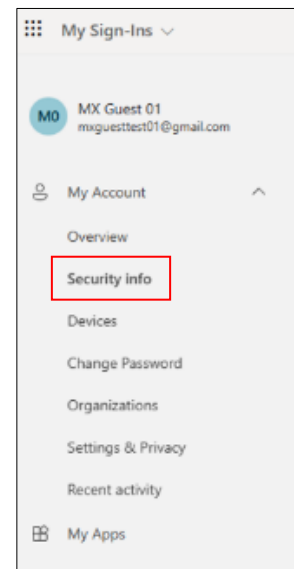
You can click  to open the full document.



The screen shown on the right will be displayed, which means that you have successfully enrolled.

5. You can close your browser. Alternatively, to confirm successful enrollment and validate that the Microsoft authentication method was added in the list of sign-in methods for your account by visiting the "Security Info" section.

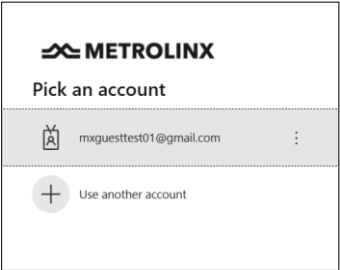
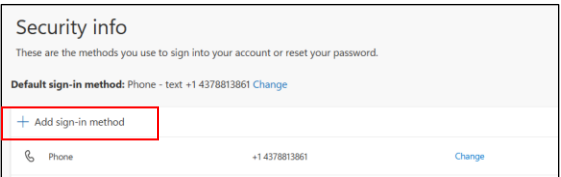
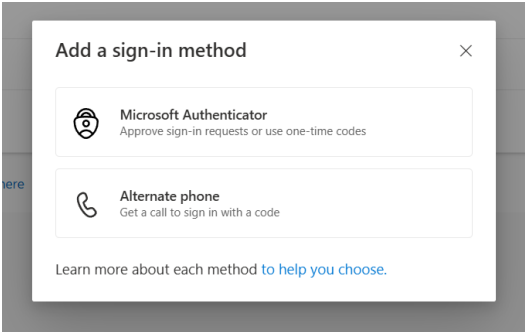
Note: You may be asked to authenticate again when visiting the "Security Info" section.



Enroll additional MFA methods (Optional)

You can enroll **multiple MFA methods**. This section outlines the process to enroll additional methods after you have already successfully enrolled with at least one method.

Sign-in to your account to enroll for additional methods or devices.

- On a computer, open the following link: https://aka.ms/mfasetup?tenant=191b00ea-edcc-406c-8456-dc29abc0f10f - Login with your email address. - Once authenticated, you will land on the Security info page.	
- Click "Add Sign-in Method" to add a new MFA method. - Select your preferred additional method and complete its registration, refer to steps above according to the MFA method (option A or B) you would like to register for your account. If you have previously enrolled for Phone (option B) as MFA method, you can add an additional phone number using "Add Alternate Phone" option. If you have previously enrolled for the Authenticator application (option A), you can enroll also enroll with a second device.	 

FAQ: Frequently Asked Questions

GENERAL QUESTIONS

1. What is Multifactor Authentication?

Multifactor Authentication (MFA) is a security feature that helps protect online accounts by requiring more than one form of verification before granting access. Traditionally, you only needed a password to sign in, but passwords can be stolen or guessed. MFA adds extra layers of protection, such as a code sent to your phone, code generated from an authentication app, or a prompt in an authentication app.

By using MFA, your accounts are much less likely to be compromised. MFA is now a common and recommended practice for organizations worldwide to keep data safe and secure. It's easy to set up and use, and it's one of the most effective ways to protect online services and data.

2. How is MFA being deployed at Metrolinx?

Metrolinx is rolling out Multifactor Authentication (MFA) to strengthen the security of online applications and to protect sensitive information. The deployment process is designed to be straightforward and supportive, ensuring all users can easily enroll and use MFA. The rollout is happening in phases, starting with a pilot consisting of a select group of users and I&IT employees starting in December 2025. This will be followed by a roll-out to all remaining internal and external users in January 2026. Support resources—including step-by-step guides, FAQs, and helpdesk assistance—will be available to help everyone through the process.

Metrolinx is using Microsoft Entra ID (formerly Azure Active Directory) as the main platform for MFA. Users will be required to register a mobile device or download an authentication app (Microsoft Authenticator). Once enrolled, you will be prompted to verify your identity with a code or approval notification when accessing protected applications, especially from new devices or locations.

Metrolinx IT and helpdesk teams will be closely monitoring the deployment, ready to assist with any technical issues. This phased approach will help minimize disruptions and ensure everyone has the support they need. The goal is to make MFA adoption as smooth as possible while significantly improving the security of Metrolinx's digital environment.

3. What are the Benefits of MFA?

Multifactor Authentication (MFA) offers several important benefits for both individuals and organizations like Metrolinx. The primary advantage is significantly improved security. By requiring two or more forms of verification—MFA makes it much harder for cybercriminals to gain unauthorized access to your accounts.

Another key benefit is the protection of sensitive data. With MFA in place, confidential information, financial records, and personal details are far less likely to be exposed in the event of a phishing attack or data breach. This helps Metrolinx maintain compliance with privacy regulations and build trust with employees and partners.

MFA also reduces the risk of identity theft and fraud. This layered approach to security is especially important for organizations that rely on cloud-based services and remote access.

4. By enrolling in MFA, will Metrolinx be able to track my device or see my activity?

MFA does not allow Metrolinx to see anything on your mobile device, track your whereabouts or your device activity. Your own privacy is protected.

5. Which applications are Microsoft Entra ID MFA-enabled and enforced?

As of March 31, 2026, access to following applications will require MFA – iSupplier, Oracle Primavera Unifier, and Oracle Aconex.

6. In which situations am I required to authenticate through MFA?

MFA will be required every time you access a protected application unless you have an existing active session from a previous login.

7. Do I need to be connected to internet for using Microsoft Authenticator?

Yes. To get sign in push notifications and to send your response your device needs to be connected to the internet.

ENROLLMENT QUESTIONS

1. Who is required to enroll for MFA?

All Metrolinx partners who are required to enroll will receive an email (from invites@microsoft.com) to sign-up and register for MFA. If you receive such an email, please enroll as soon as possible.

2. How do I enroll?

Please follow the steps described in this document.

3. What happens if I do not enroll for MFA?

As of March 31, 2026, Metrolinx will progressively begin to enforce MFA for enterprise applications. If an access attempt requires MFA and you have not yet enrolled, you will be forced to enroll for MFA before you are able to access the application. We strongly recommend you enroll as soon as possible.

4. I am having issues accessing the invitation link to start the enrollment process. To whom can I talk?

Please call Help Desk at 416-202-5000 (directory option #3) to get assistance.

5. Can I use other, non-Microsoft authenticator mobile app such as Google Authenticator?

No, only Microsoft authenticator app is supported.

6. Can Microsoft Authenticator be installed on a computer?

No, it cannot be installed on a computer. The app must be installed on an iPhone or an Android device.

7. Can I use a phone number instead of using the Microsoft Authenticator app on the mobile device?

You can use a phone number instead of the Microsoft Authenticator app. However, using the Microsoft Authenticator app is the easy, more secure, and recommended method to enroll for MFA.

8. Do I need to have a mobile device to install the Microsoft Authenticator app?

Yes, you will need a mobile device (i.e., iPhone or Android) to install Microsoft Authenticator.

9. Can I have multiple devices with Microsoft Authenticator installed?

Yes, you can install Microsoft Authenticator on multiple devices (e.g., a company or a personal mobile device).

10. If I have two devices with Microsoft Authenticator installed, will notifications come to both devices?

Yes, if you have more than one device with Microsoft Authenticator installed, both devices will receive a notification prompt when you need to complete the MFA. You will only be required to use one of the devices to approve the notification.

11. I have not been issued a mobile device from my employer. How do I enroll?

The use of personal mobile device for MFA enrollment is supported.

12. I have a new phone with the same number, and I only had Microsoft Authenticator previously registered. I can no longer use Microsoft Authenticator.

Please call Help Desk at 416-202-5000 (directory option #3) to get assistance.

13. I have a new phone with the same number. I previously registered my device for Microsoft Authenticator as well as my phone number. I can no longer use Microsoft Authenticator.

Authenticate to [Entra ID](#) and follow the instructions in this document to install and register Microsoft Authenticator on your new phone for MFA.

14. My phone was reset or wiped. I am now unable to use Microsoft Authenticator to log in. I did not register my phone number as a backup authentication method.

Please call Help Desk at 416-202-5000 (directory option #3) to get assistance.

15. My phone was reset or wiped. I am unable to use Microsoft Authenticator to log in. I have a phone number registered before my phone was reset or wiped.

Authenticate to [Entra ID](#) and follow the instructions in this document to install and register Microsoft Authenticator on your new phone for MFA.

16. I've lost my MFA configured device - How do I proceed?

Please call Help Desk at 416-202-5000 (directory option #3) immediately to report loss of MFA device and to get further assistance.