

MFA Authentication Guide

Accessing Metrolinx Resources with Microsoft Entra ID MFA and SSO

External User Guide & FAQ

February 2026

Content

Objectives and Prerequisites	1
Your Login Experience for Entra ID MFA protected applications	2
Your Login Scenarios: How are you accessing Metrolinx resources?	2
Step 1: Navigate to Your Application and Verify Your Identity	3
Step 2: Registering for Multi-Factor Authentication (MFA)	4
Step 2A: Registering with Authenticator App (Option A)	5
Step 2B: Registering with SMS or phone (Option B)	10
Step 3: Logging in with Multi-Factor Authentication (MFA)	12
Successful Login	15
Register additional MFA methods (Optional)	16
FAQ: Frequently Asked Questions	18

Objectives and Prerequisites

This guide takes you through the login process for users with a **non-Metrolinx account** to Metrolinx resources protected by Microsoft Entra ID with Multifactor Authentication (MFA).

A list of the Metrolinx applications protected by Microsoft Entra ID:

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

For all other applications not listed above, you will continue to authenticate with Okta.

Should you experience any Entra ID issues, you can contact the Help Desk for support by phone at **416-202-5000** (directory option #3).

For any application specific issues, you can contact the respective application support team at Metrolinx.

Your Login Experience for Entra ID MFA protected applications

Metrolinx is gradually transitioning its applications to Microsoft Entra ID. As this migration progresses, you will notice changes in how you log in to the following applications. However, how you navigate to your applications will not change.

Please see the table below for the applications affected and the specific login changes.

Applications	Login Changes
Microsoft Office 365 applications (Teams, SharePoint, Word, Excel, PowerPoint, Outlook, Power BI, etc.)	Switches from Okta to Microsoft Entra ID with MFA for application access. You will no longer be asked to authenticate using Okta's sign-in page.
Oracle Aconex Construction Engineering Aconex Logon	Switches from native authentication to Microsoft Entra ID with MFA. After providing your login name or work email on the Aconex login page, you will be automatically redirected to sign in via the Microsoft sign-in page.
Oracle Primavera P6 and Unifier	Switches from Oracle-managed authentication to Microsoft Entra ID with SSO and MFA. You will log in directly via the Microsoft sign-in page.
Oracle iSupplier	

Your Login Scenarios: How are you accessing Metrolinx resources?

Your login steps will vary depending on how you are accessing Metrolinx resources. Having not registered your account for MFA will impact your login process.

Login Scenario	Login Steps
My account has not been registered for MFA	1. Navigate to the application as you typically do, or use the link provided in the application table above. 2. Verify your identity (Step 1). 3. Complete the MFA registration process (Step 2) upon login for continued access to applications protected by Entra ID. Once completed, you will be automatically redirected and signed in to your application.
My account is already registered for MFA	1. Navigate to the application as you typically do, or use the link provided in the application table above. 2. Verify your identity (Step 1). 3. Login with MFA (Step 3) to your application using your account's registered method(s).

To avoid any sign-in related issues once changes are applied, you may need to restart your device.

Step 1: Navigate to Your Application and Verify Your Identity

1. Navigate to your desired application how you normally would, or use the [Login Experience Application Table](#) for a direct link to your application.



Navigate to your application

2. When accessing the Entra ID protected applications, you will need to verify your identity using one of three methods below depending on your email address.

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.

A screenshot of the Microsoft Sign in page for an organization account. The page has a white background with the Microsoft logo at the top. Below the logo, it says "Sign in" and "Email, phone, or Skype" with a red box around the input field. There are links for "No account? Create one!" and "Can't access your account?". A blue "Next" button is at the bottom right.

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.

A screenshot of the Microsoft "Enter your password" page. The page has a dark background with the Microsoft logo at the top. Below the logo, it says "Enter your password" and "Password" with a red box around the input field. There is a "Forgot your password?" link and a blue "Next" button. At the bottom, it says "Sign in with a different 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.

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. Retrieve and enter the passcode from the mailbox and click "**Sign-in**".

A screenshot of a Metrolinx email. The email is from "mxquestest01@gmail.com" and says "Sign in". It says "We'll send a code to mxquestest01@gmail.com to sign you in." and has a blue "Send code" button with a red box around it.

A screenshot of a Metrolinx email. The email is from "Metrolinx (via Microsoft)" and says "Account verification code". It says "Account verification code: 11326491" with a red box around the code. There are links for "Privacy Statement" and "Microsoft Corporation, One Microsoft Way, Redmond, WA 98052".

A screenshot of the Metrolinx "Enter code" page. The page has a white background with the Metrolinx logo at the top. Below the logo, it says "Enter code" and "We just sent a code to mxquestest01@gmail.com". There is a red box around the input field containing the code "11326491". A blue "Sign in" button is at the bottom right.

Step 2: Registering for Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is an authentication process that adds an extra layer of security when accessing your applications or systems by prompting you for both your username/password and a **second factor** (Microsoft Authenticator application or Phone number) to validate your identity.

The table below summarizes the second factor options you can use.

Option	Details	Recommended to...
2A 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
2B 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.*

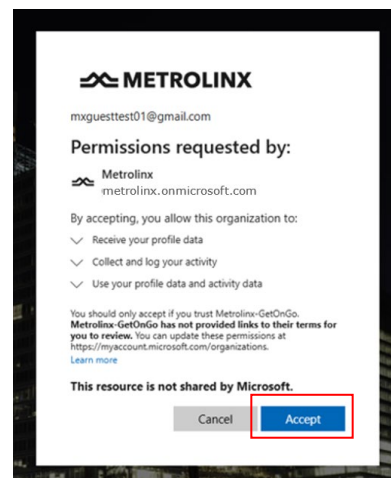
We recommend registering both MFA options to prevent future login interruptions and minimize the need for helpdesk assistance in cases where a specific MFA method is unavailable. For example, if you upgrade your mobile device and lose access to the Microsoft Authenticator app, or if you change your phone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

Step 2A: Registering with Authenticator App (Option A)

Step 2A.1: Accept permissions request

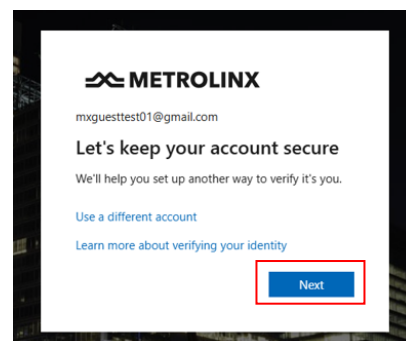
1. After having verified your identity, you may be asked to **accept** the prompt for permissions requested by Metrolinx.

If you previously accepted the permissions request, then this step would be skipped.



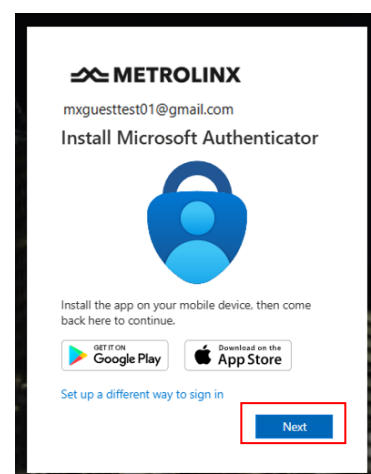
2. Click "**Next**" to begin the registration process.

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.

If you want to enroll for Phone OTP as MFA method instead of the Microsoft Authenticator app, click "**Set up a different way to sign in**" and follow the instructions in [Section 2B: Registering with SMS or phone \(Option B\)](#).

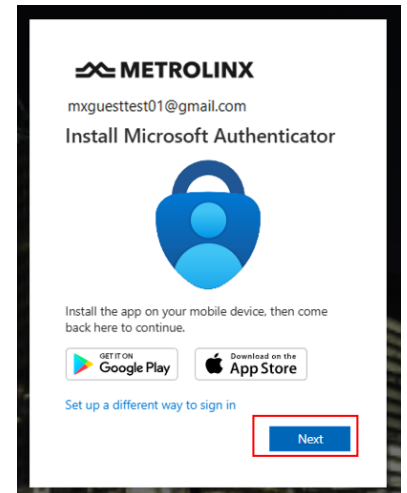


Step 2A.2: Download the Microsoft Authenticator app (if not already installed)

Note: If the Microsoft Authenticator application is already installed on your mobile device, you can skip steps 1 and 2. However, please make sure the application is updated to the latest version.

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.

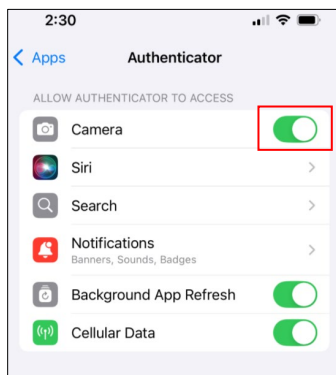
Important: when you open the Microsoft Authenticator app, **please accept and allow the Microsoft Authenticator app to send you notifications and access your camera** (please note that it does not mean that the Microsoft Authenticator app is accessing your photos). It is required to complete the enrollment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



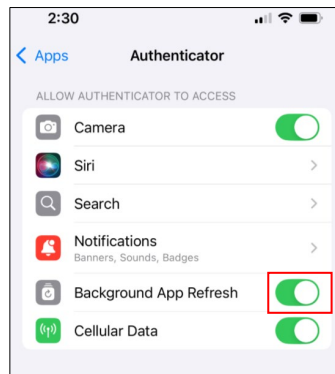
3. If the application does not have the required permission enabled, go to your mobile device phone settings app, search for "Authenticator" and enable the following permissions:

**The steps below will vary across different mobile device models and versions.*

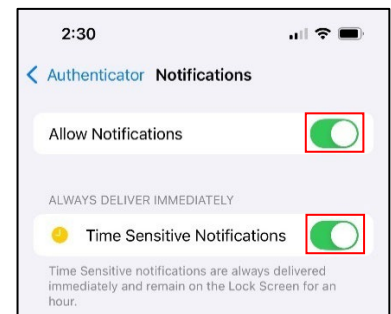
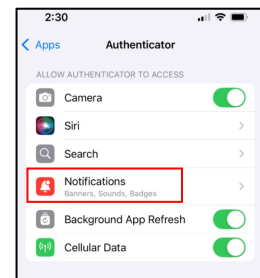
a) Allow access to camera



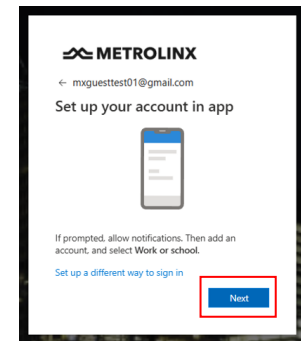
b) Enable Background App Refresh



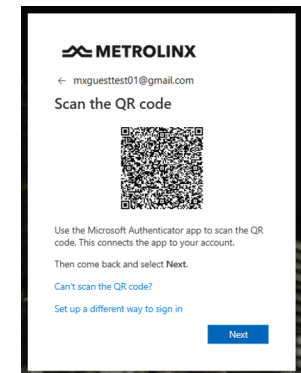
c) Allow notifications



- 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.



- A QR code screen will be displayed on your computer to add your account in the Authenticator application, proceed to the next section. Do not click "**Next**" as you will need to scan the QR code with your mobile device.

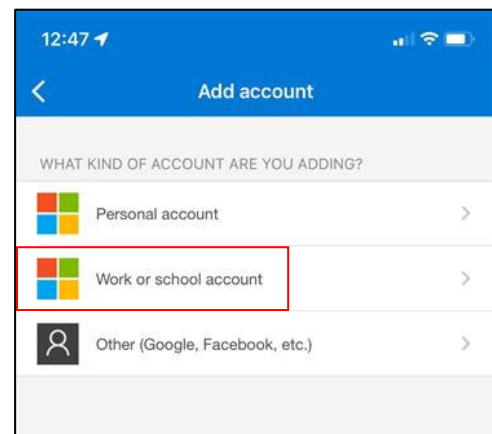


Step 2A.3: Add your account in the Authenticator application

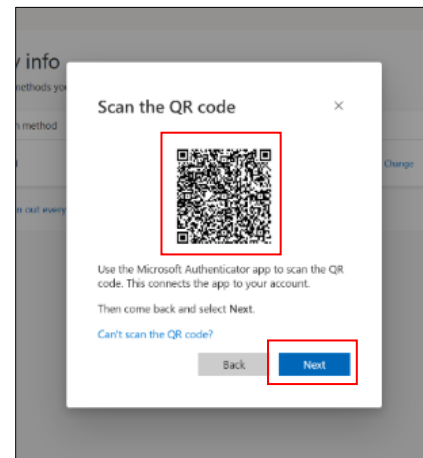
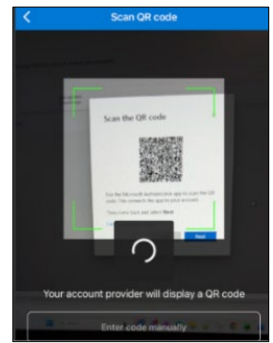
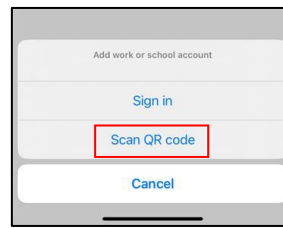
- On your mobile device, open the Microsoft Authenticator application. You may be presented information explaining the app, select "**Skip**".
- Click "**Add an account**" (or click on the + in the right-hand corner if it is not the first time that you add an account to Microsoft Authenticator app).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

- Select "**Work or school account**".
- If you are using the 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**".



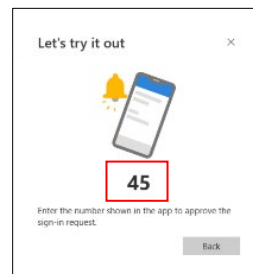
6. Click "**Scan QR Code**" and **scan the QR code** displayed on your computer screen using the mobile device camera. This will add your Metrolinx account to your Microsoft Authenticator application on your mobile device.
7. On your computer screen, only after you have scanned the QR code, click "**Next**" and wait until the system has finished checking the activation status.



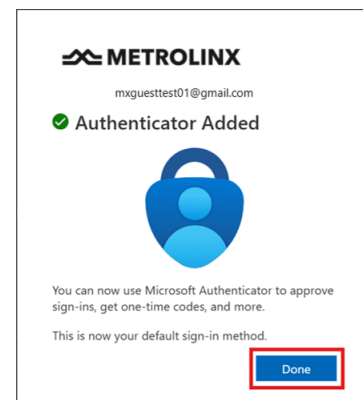
Step 2A.4: Complete the Authenticator app enrollment process

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

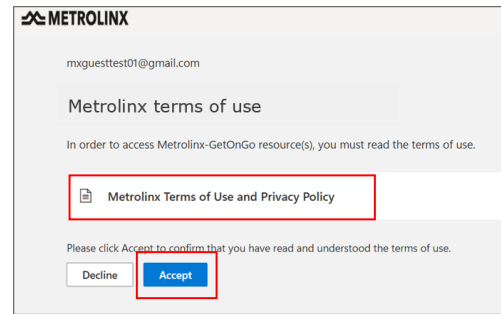
1. Enter the number displayed on your computer screen in your mobile device and click "**Yes**".



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**".



4. Accept the Terms of Use and Privacy Policy by **clicking** the document box to read and "**Accept**".



After successfully registering, you will be granted access to your application. For a screenshot of what a successful login to each application looks like, refer to the [Successful Login](#) Section.

For any issues authenticating into your application via Entra ID, refer to the [FAQ](#) section.

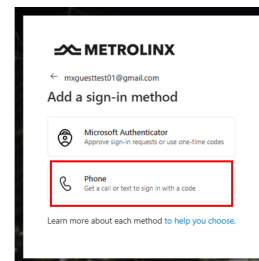


Successful MFA Login

Step 2B: Registering with SMS or phone (Option B)

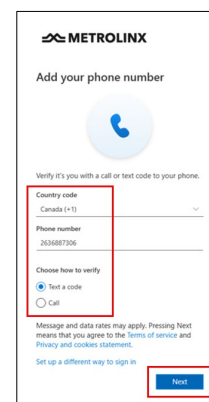
Step 2B.1: Provide your phone number

1. Click **"Phone"** as your MFA method you would like to add.



2. Enter your **phone number country code** and phone number to be used as MFA method
3. **Select** verification method: SMS or Phone call.
4. Click **"Next"**.

The phone number entered should be a number you have access to and can use to authenticate yourself with.



Step 2B.2: Complete the phone enrollment process

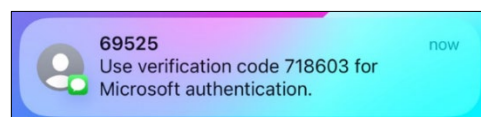
5. You will receive a verification code by SMS or by phone call (according to the method selected in the previous step) on your mobile device.

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 receive 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.*

6. 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?".



<i>The screen shown on the right will be displayed, indicating that the verification was successful.</i> 7. Click "Done".	 A screenshot of a Metrolinx mobile application screen. At the top is the Metrolinx logo. Below it, a green checkmark icon is followed by the text 'Phone number added'. In the center is a large blue circular icon with a white telephone handset. At the bottom, there is a small text line 'You can now receive a code each time you sign in.' and a blue button labeled 'Done' which is highlighted with a red rectangular box.
8. Accept the Terms of Use and Privacy Policy by clicking the document box to read and "Accept".	 A screenshot of a Metrolinx mobile application screen titled 'Metrolinx-GetOnGo terms of use'. It shows the email 'mxguesttest01@gmail.com' and a document icon next to the text 'Metrolinx Terms of Use and Privacy Policy', which is highlighted with a red rectangular box. At the bottom, there are two buttons: 'Decline' and 'Accept', with the 'Accept' button highlighted by a red rectangular box.
After successfully registering, you will be granted access to your application. For a screenshot of what a successful login to each application looks like, refer to the Successful Login Section. For any issues authenticating into your application via Entra ID, refer to the FAQ section.	 A large black checkmark icon is centered at the top. Below it, the text 'Successful MFA Login' is centered in a bold, black font.

Step 3: Logging in with Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is an authentication process that adds an extra layer of security when accessing your applications or systems. After entering your username and password, you will be prompted to verify your identity using a **second factor already registered to your account**, such as the **Microsoft Authenticator app** or a code sent to your **mobile device** via phone call/SMS.

Instead of relying solely on your password, MFA helps protect your account by requiring this additional verification step each time you log in.

1. After [verifying your identity](#), complete the multi-factor authentication using one of the second factors you would have already registered to your account:

- To use the [Authenticator application](#), refer to **method 1**.
- To use the verification code by [phone call](#), refer to **method 2**.
- To use the verification code by [SMS](#), refer to **method 3**.

**The steps outlined in each method will vary across different mobile device models and versions.*

For **method 1**, using the [Microsoft Authenticator application](#):

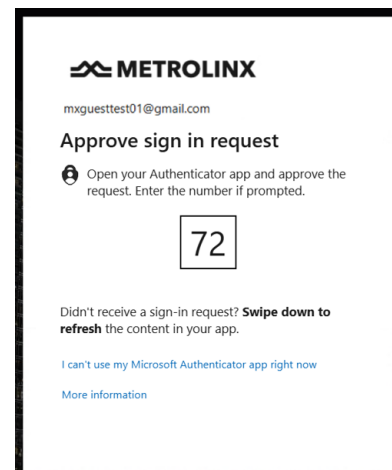
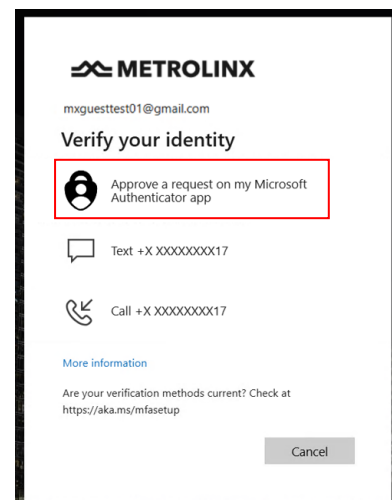
Make sure your mobile device is connected to the internet.

Click on the Authenticator app option to verify your identity.

To approve your sign-in request, a number will be displayed on your screen, which you must enter in your authenticator app (a notification may be triggered on your phone for ease of use).



Once completed, your sign-in request will be approved, and you have completed your authentication.



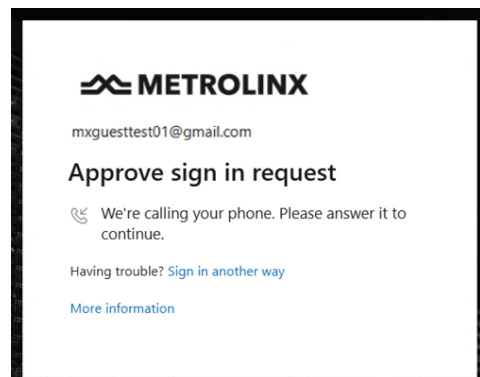
For **method 2**, using verification code via phone call:

Click on the option to "Call +X XXXXXXXX17" your phone number registered to the account you are using to login.



Answer the phone call and follow its instructions to approve your sign-in request.

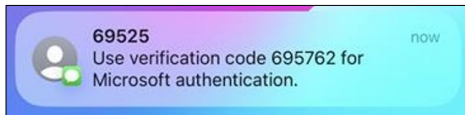
Once completed, your sign-in request will be approved, and you have completed your authentication.



For **method 3**, using verification code via SMS:

Click on the option to "Text +X XXXXXXXX17" your phone number registered to the account you are using to login.

You will receive a verification code on your mobile phone.



Enter the verification code sent to your mobile device on the Entra ID login page and click "Verify" to authentication yourself.



After successfully authenticating, you will be granted access to your application. For a screenshot of what a successful login to each application looks like, refer to the [Successful Login](#) Section.

For any issues, refer to the [FAQ](#) section.



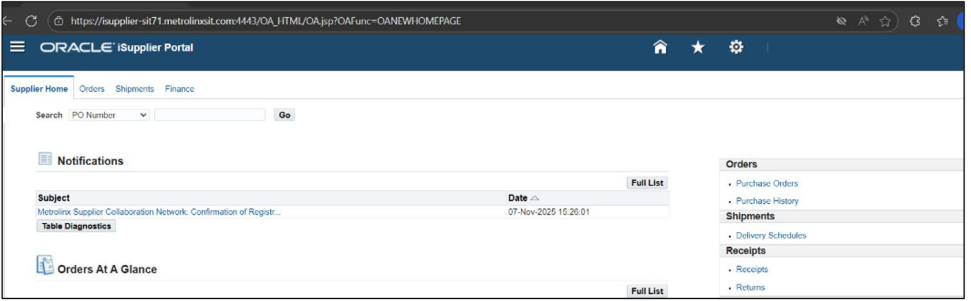
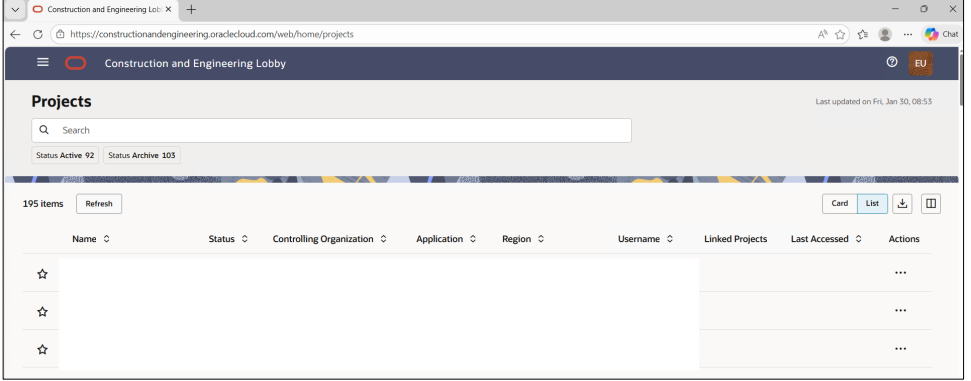
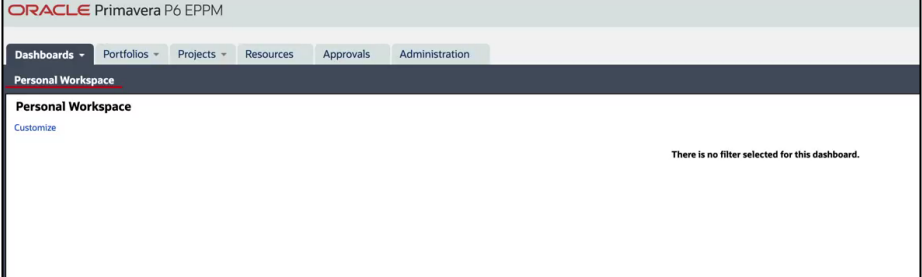
Successful MFA Login

*If you are unable to complete **one** of the many verification methods you are being asked to complete, you can manage your registered MFA methods from the [Security Info](#) page in your Entra ID profile.*

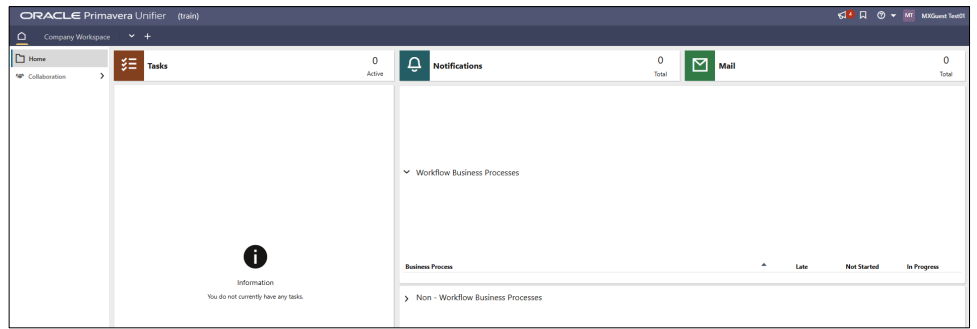
*If you are unable to complete **any** of the verification methods required, contact the Metrolinx Help Desk for assistance by phone at: 416-202-5000 (directory option #3).*

Successful Login

This section displays the completion of a successful SSO or MFA login of the Microsoft Entra ID protected applications. **Although the login process has changed, the applications have not.**

Microsoft Office 365 applications (Teams, Word, Excel, PowerPoint, Outlook, Power BI, etc.)	
Oracle iSupplier	
Oracle Aconex <i>*For signing in, you will need to first provide your login name or work email on the Oracle Aconex login page before authenticating with Microsoft Entra ID.</i>	
Oracle Primavera P6	

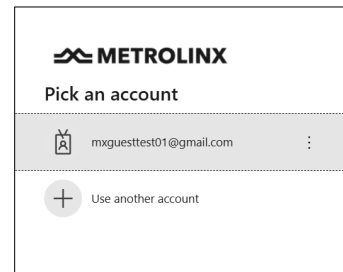
Oracle Primavera Unifier



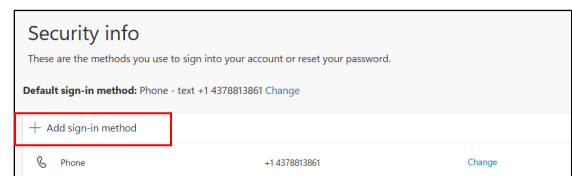
Register additional MFA methods (Optional)

You can register **multiple MFA methods**. This section outlines the process to register additional MFA methods you can use, after having already successfully registered at least one method.

1. On a computer, open go to the [Security Info](#) page of your Metrolinx Microsoft Entra ID profile.
2. Login with the email address you use to access Metrolinx resources.
3. Once authenticated, you will land on the Security info page.

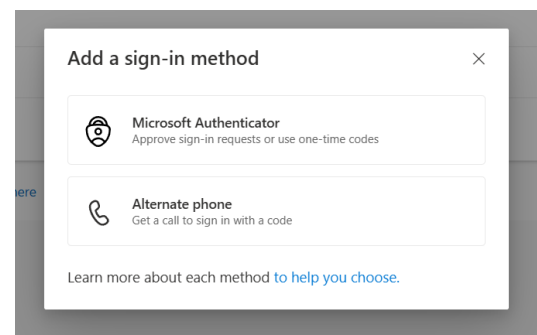


4. Click "Add Sign-in Method" to add a new MFA method.
5. Select your preferred additional method and complete its registration, refer to steps above according to the MFA method (option A or B) you would like to register for your account.



- If you 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 **register a second mobile device**.

Once you have added your additional MFA method, close the browser window.



FAQ: Frequently Asked Questions

GENERAL QUESTIONS

1. What is Microsoft Entra ID?

Microsoft Entra ID is Metrolinx's latest cloud-based identity and access management service. It is designed to help Metrolinx securely manage and control access to our resources and company applications using Single Sign-On and Multi-Factor Authentication.

2. What is Multi-Factor 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.

3. Why do I need Multi-Factor Authentication?

In alignment with our ongoing commitment to cybersecurity and public trust, Metrolinx is migrating its applications and resources to Microsoft Entra ID as its primary identity provider. As a result, Microsoft Office 365 applications (Teams, Outlook, Word, and others) and select Oracle applications will switch to using Microsoft Entra ID. However, access to all other applications not listed in this document will continue using the same authentication method as they currently do until informed otherwise.

4. Will I have to continue using Okta?

Yes, you will continue using Okta for access to all other applications that have not yet migrated to Entra ID. All applications not listed in this document will continue using the same authentication method as they currently do until informed otherwise.

5. What if I did not register my account for MFA?

If you have not registered your account for MFA, you will be forced to register your account when attempting to access any of the Microsoft Entra ID protected applications once they have been migrated to Entra ID.

MFA REGISTRATION QUESTIONS

1. 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.

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

No, only the Microsoft authenticator app is supported.

3. 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.

1. 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.

2. 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.

3. 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).

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

Yes, to receive sign-in push notifications and to send your response, your device needs to be connected to the internet.

MFA LOGIN QUESTIONS

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

MFA will be required each day you access a Microsoft Entra ID protected application.

2. Why am I being asked to register an MFA method when logging into an application?

In alignment with our ongoing commitment to cybersecurity and public trust, Metrolinx is migrating its applications and resources to Microsoft Entra ID as its primary identity provider. As a result, Microsoft Office 365 applications (Teams, Outlook, Word, and others) and select Oracle applications will switch to using Microsoft Entra ID. However, access to all other applications not listed in this document will continue using the same authentication method as they currently do until informed otherwise. For instructions on completing your MFA registration, refer to the [MFA Registration](#) section of this document.

3. Why am I having trouble accessing my application(s)?

There are multiple reasons. If you are being asked to “Keep your account secure” by registering for MFA, then please complete the registration process outlined in the [MFA Registration](#) section of this document.

For any other issues after completing the registration, contact the Help Desk for support by phone at 416-202-5000 (directory option #3)

4. Can I change the second verification factor (Phone/Authenticator app) I am being asked to complete when logging into an application?

Yes, you can change the default second factor method in the Microsoft Entra ID Portal from [Security Info](#) page. However, you can only choose from the methods already registered to your account. For instructions, refer to the *Changing MFA Settings Guide*.

To register additional authentication methods to your account, you can also use the [Security Info](#) page and refer to the [Register additional MFA methods](#) section of this document.

5. What if I no longer have access to my second factor (Phone/Authenticator app)?

If you have multiple factors, such as a Phone or Authenticator app, registered to your account of which you can still use, then you can modify your methods in the Microsoft Entra ID Portal from [Security Info](#) page. For instructions, refer to the *Changing MFA Settings Guide*.