

# Multi-Factor Authentication (MFA)

## WHAT IS MFA?

MFA stands for Multi-Factor Authentication. It is a two-step verification method of authentication.

MFA is to be enabled on all Unitec staff accounts. Staff must have access to a mobile phone to access Office 365 products off-site. This can be either a Unitec provided mobile phone or a personal mobile phone.

While in the office, you should not receive any prompts for you to enter a code sent to your mobile

By contrast, the use of a username and password combination is considered single-factor authentication.

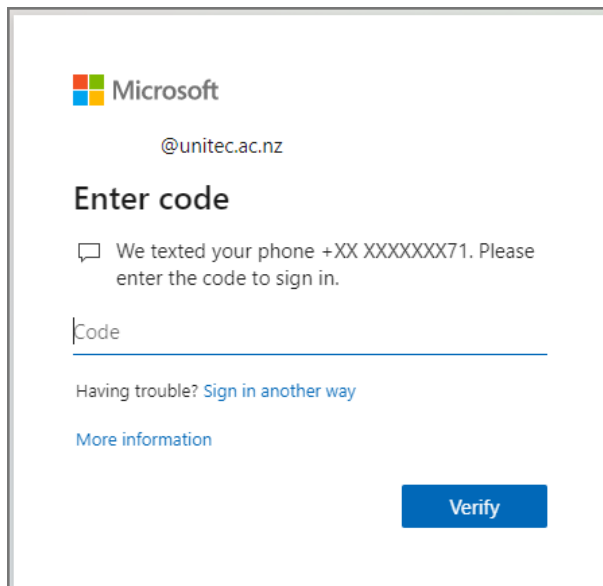
## WHY MFA?

MFA is being implemented to help protect access to Unitec Office 365 services such as Outlook, OneDrive, and SharePoint. MFA provides an additional layer of security by providing a secondary authentication process when signing into your Unitec account when you are off-campus.

If someone managed to steal your username and password, they would not be able to access our systems because they would not be able to provide the necessary verification code.

### ***Important:***

When trying to access the Unitec network from any other location (**other than Unitec Campus**), you will be asked to enter a verification code (via a Window like the one below) sent to your mobile phone.



Microsoft

@unitec.ac.nz

### Enter code

☐ We texted your phone +XX XXXXXXX71. Please enter the code to sign in.

Code

Having trouble? [Sign in another way](#)

[More information](#)

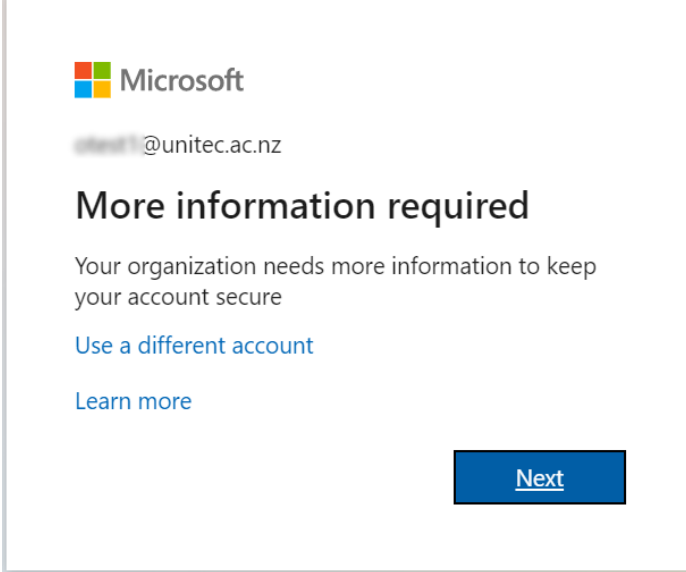
Verify

When using Office 365 **on campus**, you will **not** normally be asked for a verification code (unless you try to change the security settings).

## 1 INITIAL SET-UP

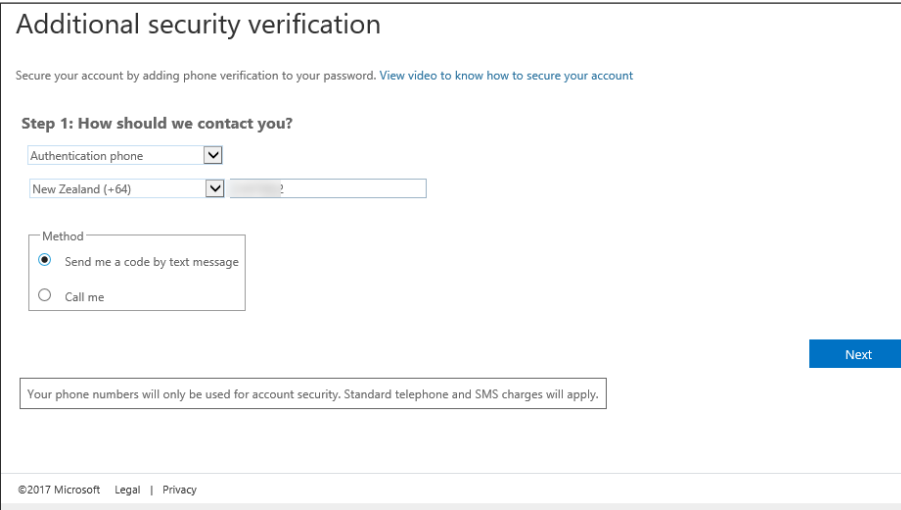
1. From an internet browser, sign in to <https://portal.office.com> with your Unitec email address, and password on your regular Unitec desktop or laptop like you normally do.

After you choose **Sign in**, you should see the following window (if you don't, you may have already set-up your security information click [here](#) to review your MFA settings).



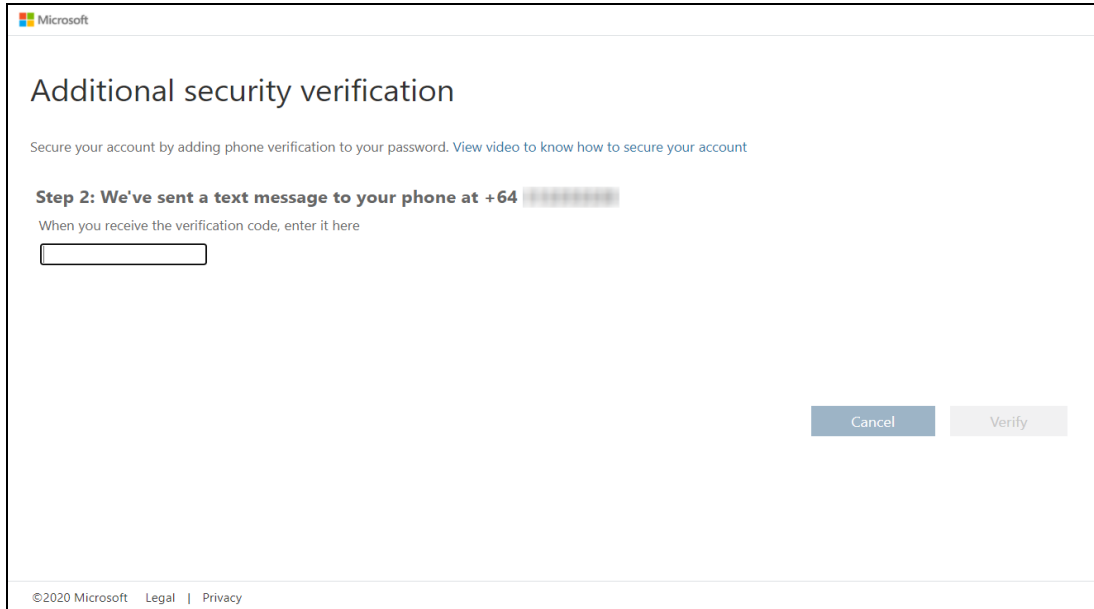
The screenshot shows a Microsoft login screen. At the top is the Microsoft logo. Below it is a blurred email address followed by '@unitec.ac.nz'. The main heading is 'More information required'. Below this, it says 'Your organization needs more information to keep your account secure'. There are two links: 'Use a different account' and 'Learn more'. At the bottom right is a blue button labeled 'Next'.

2. Click **Next**.
3. Enter your mobile phone number at the following window and click Next.



The screenshot shows the 'Additional security verification' screen. The title is 'Additional security verification'. Below it is a link: 'Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)'. The section is titled 'Step 1: How should we contact you?'. There are two dropdown menus: 'Authentication phone' and 'New Zealand (+64)'. Below these is a 'Method' section with two radio buttons: 'Send me a code by text message' (selected) and 'Call me'. At the bottom right is a blue button labeled 'Next'. At the bottom left is a small text box: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.' At the very bottom is a footer: '©2017 Microsoft Legal | Privacy'.

4. Type in the code that was sent to your mobile at the following window:



Microsoft

## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

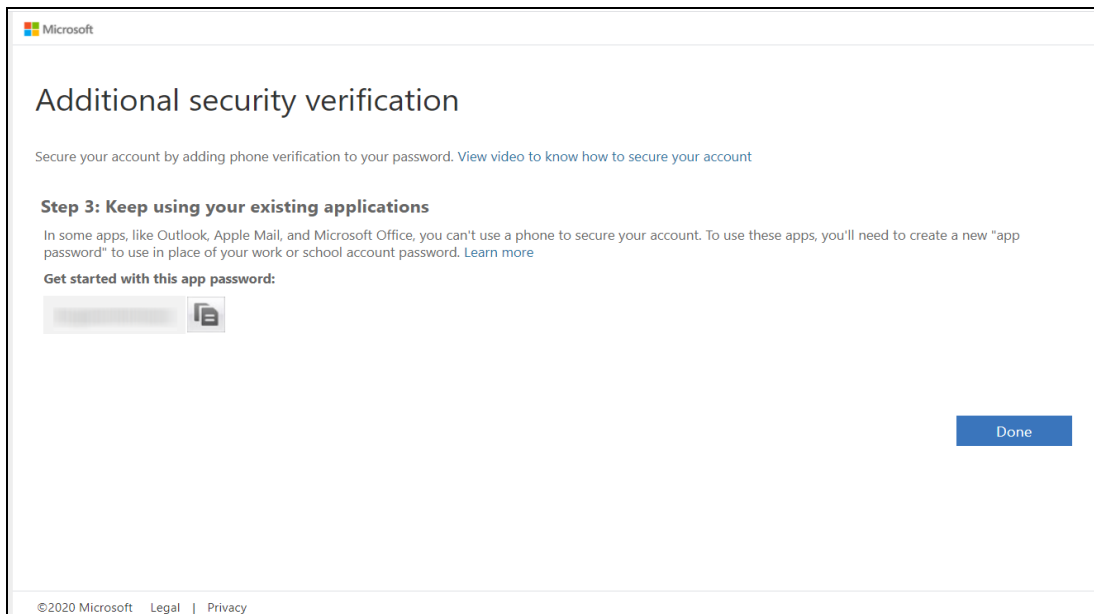
**Step 2: We've sent a text message to your phone at +64** [REDACTED]

When you receive the verification code, enter it here

Cancel Verify

©2020 Microsoft Legal | Privacy

5. Click **Done** at the following Window.



Microsoft


## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

**Step 3: Keep using your existing applications**

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. [Learn more](#)

**Get started with this app password:**



Done

©2020 Microsoft Legal | Privacy

## 2 COMMON QUESTIONS

---

### 2.1 WILL I GET PROMPTED FOR MFA EVERY TIME I SIGN IN?

You will not get prompted when you are logged on from the Unitec network (Mt Albert and Waitakere Campuses). If you use Chrome and/or Firefox browsers, you will be prompted for a code when you are at home or other remote locations. The Outlook App, Microsoft Edge, and Internet Explorer browsers on a Unitec managed laptop will not prompt for a code.

### 2.2 WHAT IF I FORGET OR RESET MY PASSWORD?

You will be sent a verification code to your Authorized phone as is current practice. After you reset a password, you should be able to continue using all apps on that device.

### 2.3 WHAT IF I DON'T HAVE MY PHONE WITH ME?

You will **not** be able to access Office 365 services like Outlook, SharePoint when **off** campus without the Verification Code sent to your Authorized Phone.

### 2.4 WHY AM I NOT GETTING A CODE SENT TO MY PHONE?

Check the notification settings on your mobile phone and enable them so that your phone calls, messaging app, or Authenticator app sends alerts. Push notifications are not required, but they help you complete the verification method in a timely way.

If this continues to be a problem, we recommend installing the use of the mobile Authenticator App. See [Alternative Verification Method](#)

### 2.5 WHAT IF I HAVE A PROBLEM WHILE TRAVELLING?

If you're travelling, the easiest verification method to use is **Microsoft Authenticator App**. It's just one click instead of typing in a 6-digit code. And, you won't incur roaming fees when you use it.

See [Alternative Verification Method](#)

### 2.6 CAN SOMEBODY ELSE USE MY CODE?

No. A person can only authenticate to applications protected by 2FA if they know your login credentials and have physical access to your smartphone.

### 2.7 I DON'T HAVE A WORK PHONE AND DO NOT WANT TO USE MY PERSONAL PHONE. HOW CAN I USE MFA?

You have to talk to your manager about a work phone; otherwise, you cannot use MFA.

## 2.8 WHAT IF MY SMARTPHONE IS LOST OR STOLEN?

Please log a call with the Service Desk to have your security information updated.

## 2.9 CAN I REGISTER MY SMARTPHONE WITHOUT USING A QR CODE?

Yes, in the Authenticator app, you have the option to log into your Microsoft account.

## 2.10 I HAVE SET UP MFA ON MY MOBILE BUT DO NOT HAVE IT WITH ME. NOW WHAT?

You cannot use MFA. Please log a call with the Service Desk as fast as possible to update your security information.

## 2.11 WHAT HAPPENS IF I CHANGE MY PHONE NUMBER?

You need to update your security information to register the new phone number. Go to <https://aka.ms/mfasetup> to do this; otherwise, contact the Service Desk for assistance.

## 2.12 I ACCIDENTALLY DELETED MY MFA APP. WHAT SHOULD I DO?

Re-install the Authenticator app and go through the set-up process again.

## 2.13 CAN I ACCESS MY UNITEC ACCOUNT FROM OVERSEAS?

If you are working overseas, you will need approval from HR and IT, as some applications and systems may not be available.

# 3 ALTERNATIVE VERIFICATION METHOD


---

An alternative verification method you may consider setting up is **Microsoft Authenticator app**. It's the easiest verification method to use as it's just one click instead of typing in a 6-digit code.

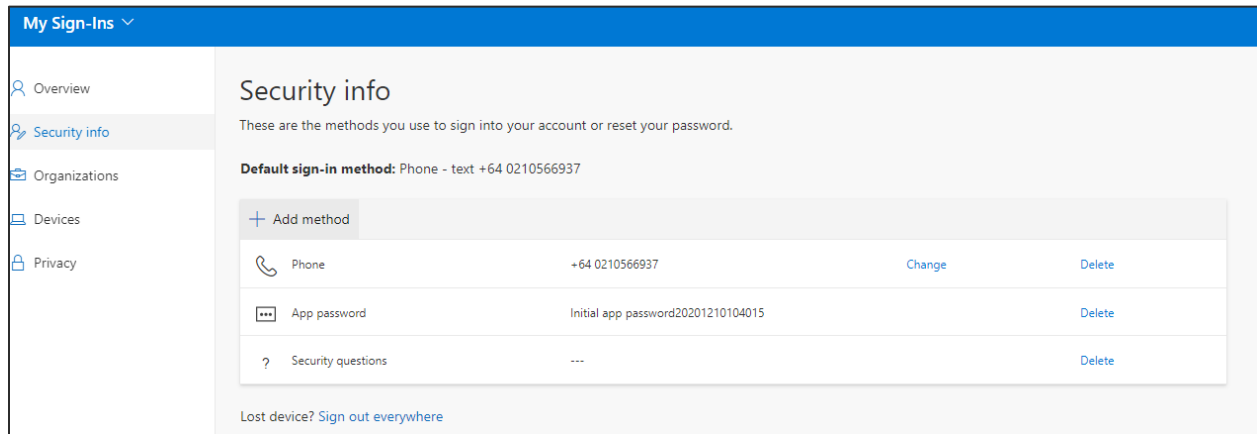
Download and install the Microsoft Authenticator app

Download and install the Microsoft Authenticator app for [ANDROID](#), [IOS](#), or [WINDOWS PHONE](#).

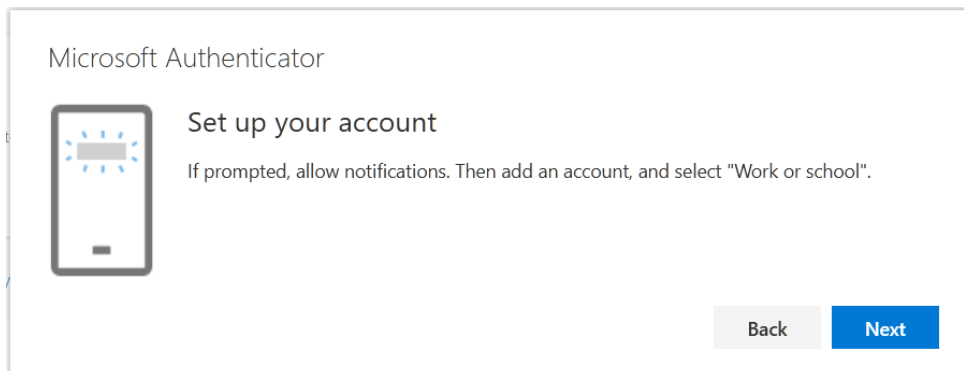
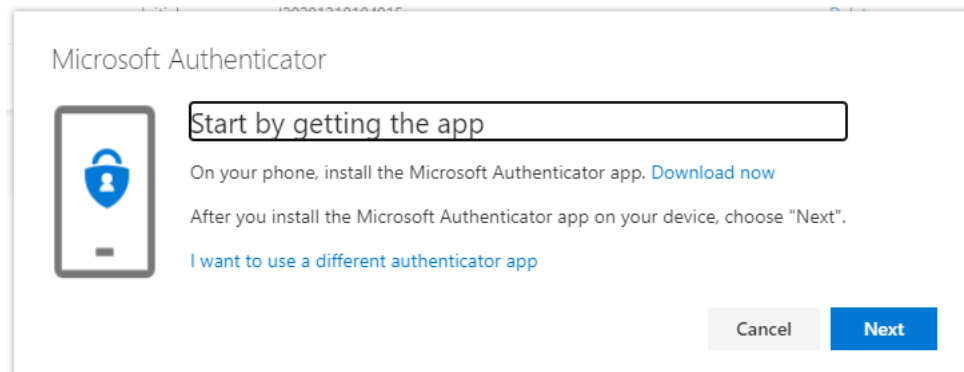
## 3.1 SET UP THE MICROSOFT AUTHENTICATOR APP

1. Choose **Settings**  > **Office 365**.
2. Choose **Security & Privacy** > **Additional security verification** > **Update my phone numbers used for account security**.
3. In the drop-down box under **What's your preferred option**, choose **Notify me through the app** (This step allows you to make this the default authenticator method. It is *optional*.)

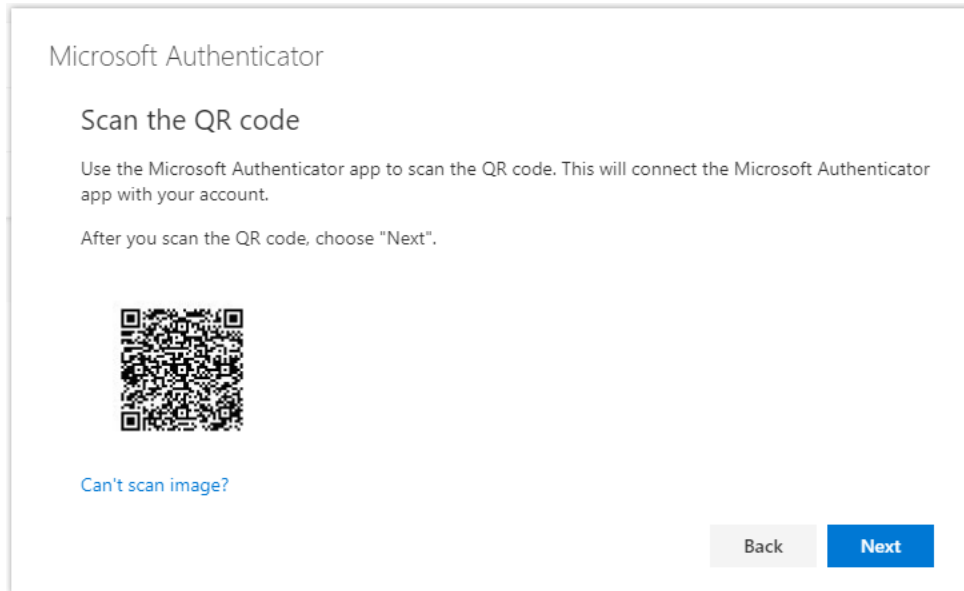
4. Check the box for the **Microsoft Authenticator** app, click **Configure**.



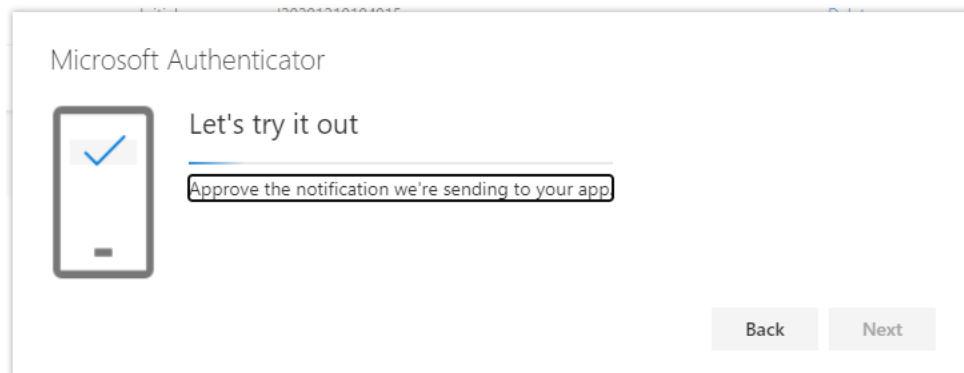
Click on "Add method."



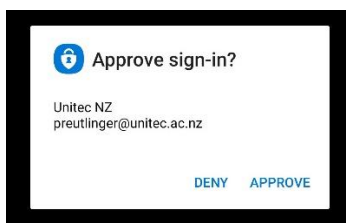
Use Scan a QR code as the easiest way to complete the set-up.

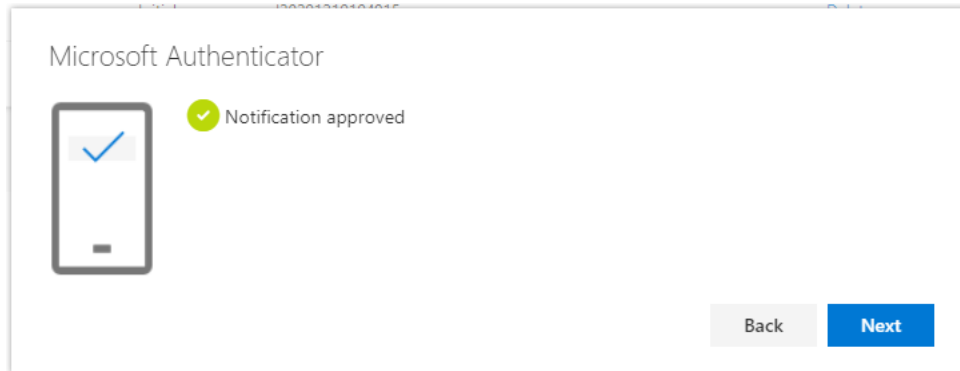


In the Authenticator app, you receive a message that you have been set up.



In the Authenticator app, the following pop-up screen appears:



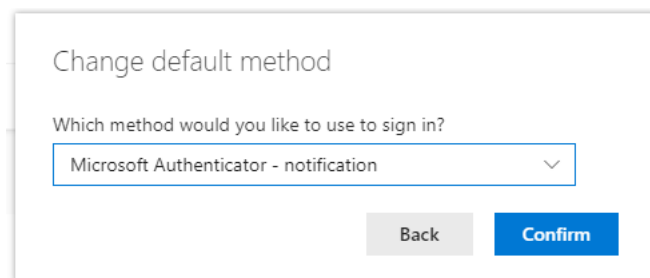


You are sent back to your Security Information Home page.

Your default sign-in method is still on text message.

**Default sign-in method:** Phone - text +64 0210566937 [Change](#)

But you can click on the “Change” link to change it to the Authenticator app.



After clicking Confirm, you are back to the Security Overview page and see the change.

**Default sign-in method:** Microsoft Authenticator - notification [Change](#)

#### More Information:

<https://support.office.com/en-us/article/Use-Microsoft-Authenticator-with-Office-365-1412611f-ad8d-43ab-807c-7965e5155411?ui=en-US&rs=en-US&ad=US>

<https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/microsoft-authenticator-app-how-to>