

Tribe User Guide Team Member with WFM Multifactor Authentication Guide

FAQ's

What's changing and why?

We've heard your feedback that having to reset your Dayforce password every 60 days is frustrating and makes it hard to remember your login details. This has caused problems with accessing rosters, timesheets, payslips, and other important information.

To make things easier:

- We're removing the need to change your password every 60 days, meaning you shouldn't have to change your password (except if it is compromised).
- Instead, we'll introduce multi-factor authentication (MFA), which means you'll use your password and then a code sent to your phone, email or an app to log in.
- You'll also be able to use biometrics (like Face ID, fingerprint or your persona device's pin code) for faster and easier access.

These changes are designed to save you time, reduce password issues, and keep your information secure.

What is Multi-Factor Authentication (MFA) and why do we need to use it?

Multi-Factor Authentication (MFA) is an extra layer of security that requires two ways to verify your identity, usually via something you know, such as your password and something you have, such as a code from your phone. We use it because passwords can be stolen or guessed, and using MFA makes it much harder for anyone else to access your sensitive information like pay, bank details and personal data.

Think of it like locking your front door and having an alarm system. One layer is good, two layers make it much safer. We care about making sure that your sensitive personal information, and your pay is extra protected.

What do I do if my phone number or email changes?

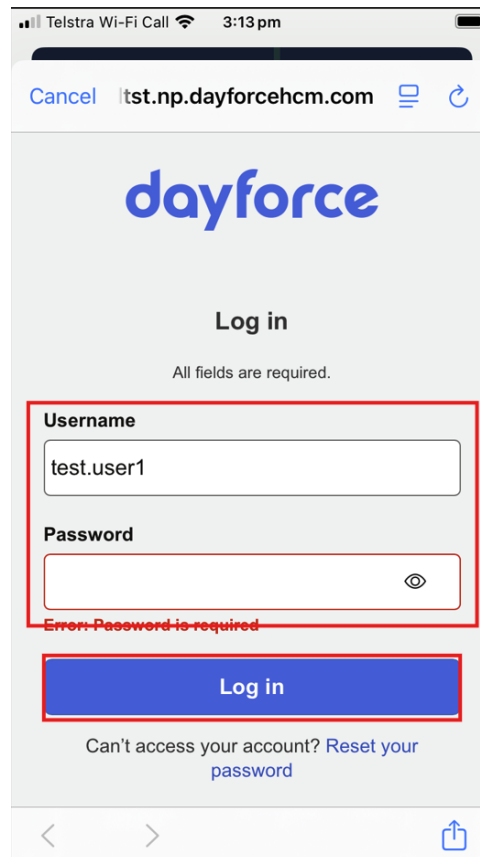
If these details change, simply follow the steps in section 2. Please also remember to update your contact details in your employee profile as well.

What if I can't get into Tribe to reset my MFA?

In these instances our team can support you to reset your MFA. To do this, please contact the People & Culture Team via email to hr@ingeniacommunities.com.au or via phone on 1300 536 518.

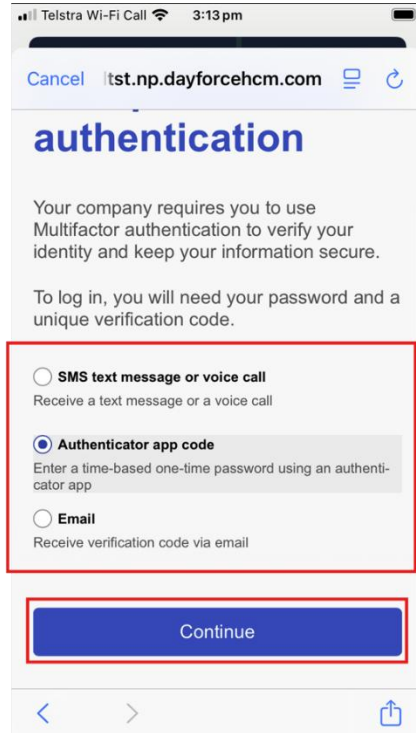
Setting up MFA – Mobile App

1. From the login page enter the company ID which is **Ingenia**, then enter your username and password. The click **Log In**.



2. From here the Multifactor Authentication setup page will appear. You will have a choice of three authentication options:
 - **SMS Text Message or Voice Call:** Set up MFA using your mobile device. A 6-digit code will be sent to your mobile device through either a text message or a voice call. This code is used to verify your identity when you log in to Dayforce.
 - **Authenticator App Code:** Set up MFA using an authentication app of your choice (e.g. Microsoft Authenticator, Google Authenticator etc). A time-based one-time password will be generated by your authentication app that you use to log in to Dayforce.
 - **Email:** Set up MFA using an email address of your choice. A time-based one-time password will be sent to your email that you use to log in to Dayforce.

3. Select the authentication method you want to use and click **Continue**.



Cancel | tst.np.dayforcehcm.com

authentication

Your company requires you to use Multifactor authentication to verify your identity and keep your information secure.

To log in, you will need your password and a unique verification code.

☐ **SMS text message or voice call**
 Receive a text message or a voice call

☒ **Authenticator app code**
 Enter a time-based one-time password using an authenticator app

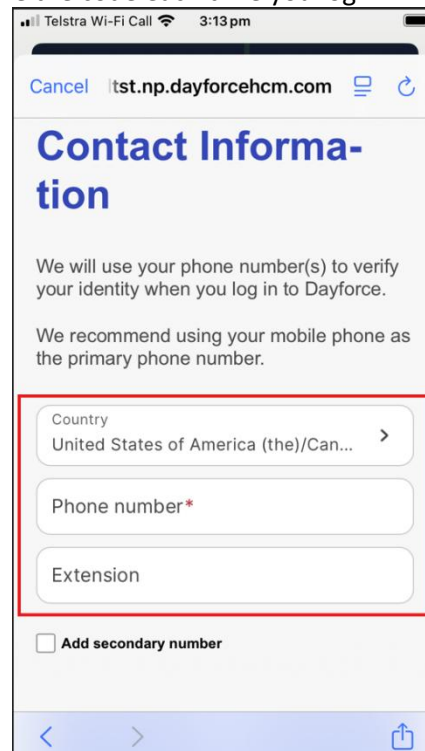
☐ **Email**
 Receive verification code via email

Continue

Set Up Multifactor Authentication Using the SMS Text Message or Voice Call Option

1. After selecting **SMS Text Message or Voice Call** in the Multifactor Authentication Setup dialog box, you're prompted to set up your contact information to receive verification codes by text message or voice call.

In the **Contact Information** dialog box, select your country and enter the primary phone number where you want to receive the code each time you log in.



Cancel | tst.np.dayforcehcm.com

Contact Information

We will use your phone number(s) to verify your identity when you log in to Dayforce.

We recommend using your mobile phone as the primary phone number.

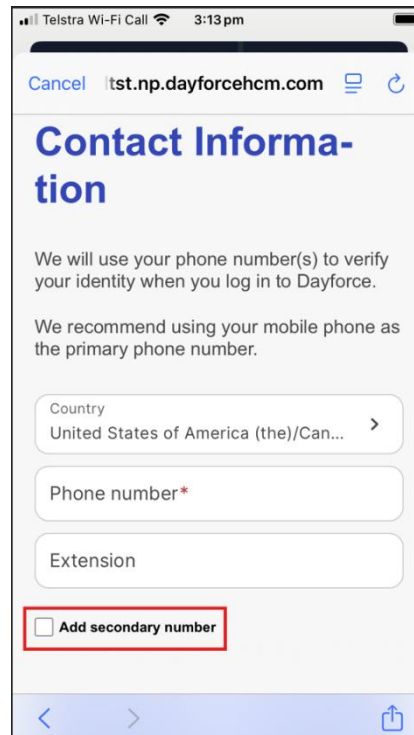
Country
 United States of America (the)/Can... >

Phone number*

Extension

☐ Add secondary number

- (Optional) Select the **Add Secondary Number** checkbox to include a back-up phone number.



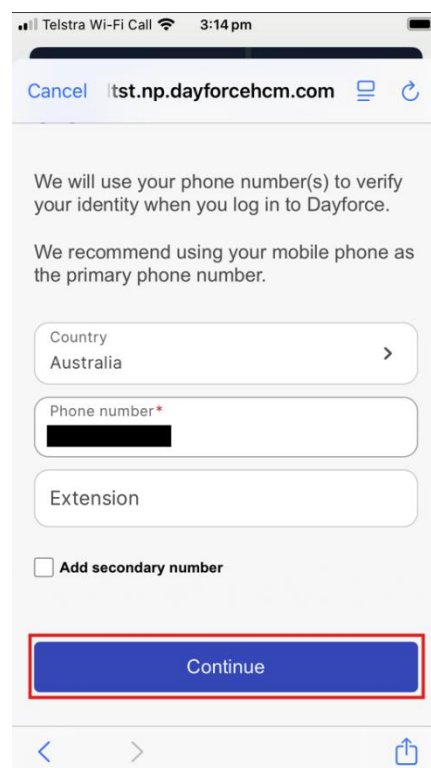
Country
United States of America (the)/Can...

Phone number*

Extension

☐ Add secondary number

- Click **Continue**.



Country
Australia

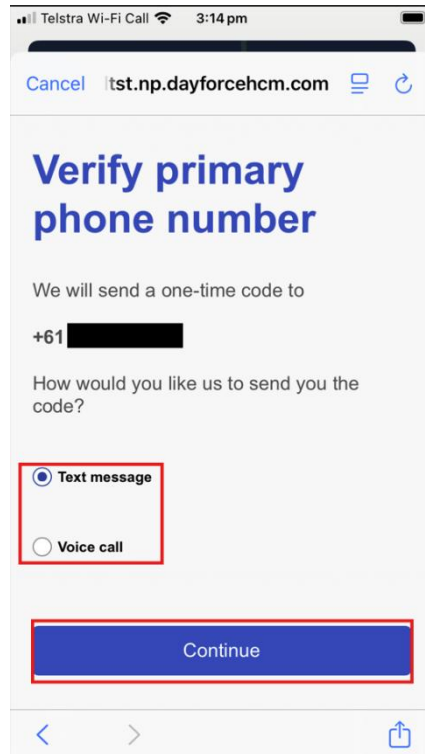
Phone number*

Extension

☐ Add secondary number

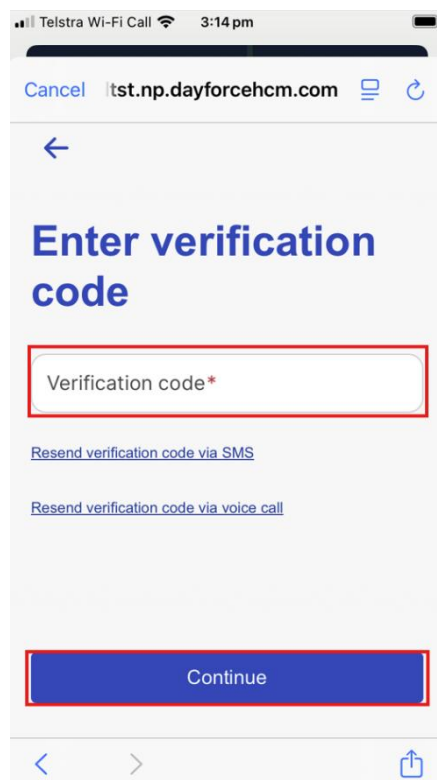
Continue

4. Select **Text Message** or **Voice Call** to indicate how you want to receive the code to verify your primary number, then select **Continue**.

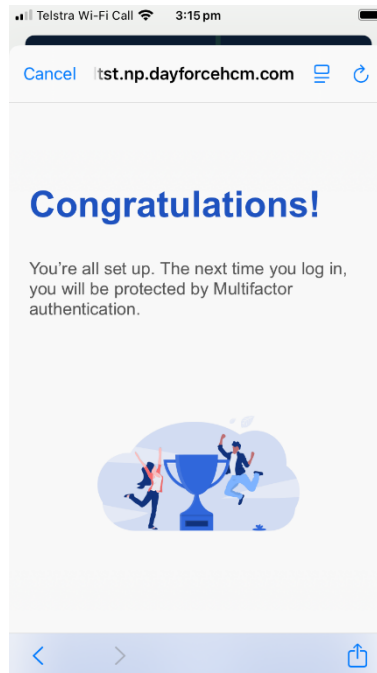


5. Enter the verification code that you received and click **Continue**. If you didn't receive a code, click **Resend Verification Code via SMS** or **Receive Verification Code via Voice Call** to try again.

NOTE: If you selected the Add Secondary Number checkbox when setting up your contact information, you will be prompted to enter and verify the secondary number.



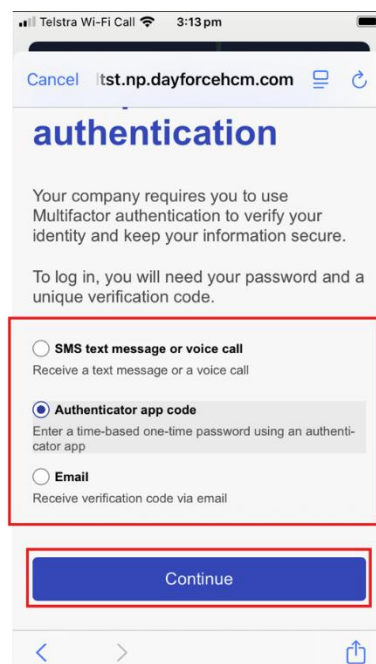
6. Your MFA setup is complete when the completion screen displays.



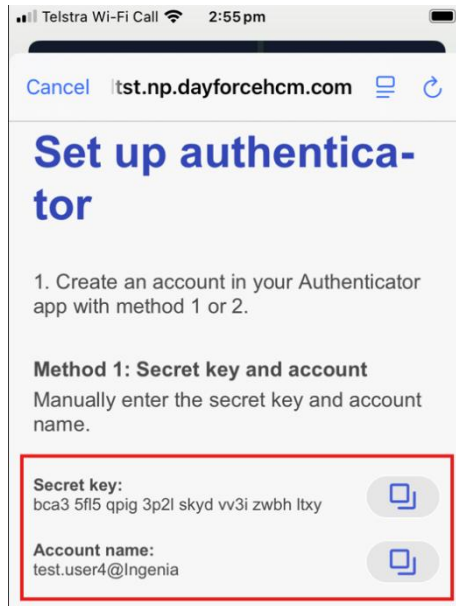
Set Up Multifactor Authentication Using the Authenticator App Option

1. After selecting **Authenticator App Code** in the **Set up Multifactor Authentication** screen, you are prompted to set up the authenticator. This option lets you receive time-based one-time verification codes through the authenticator app instead of text messages or voice calls.

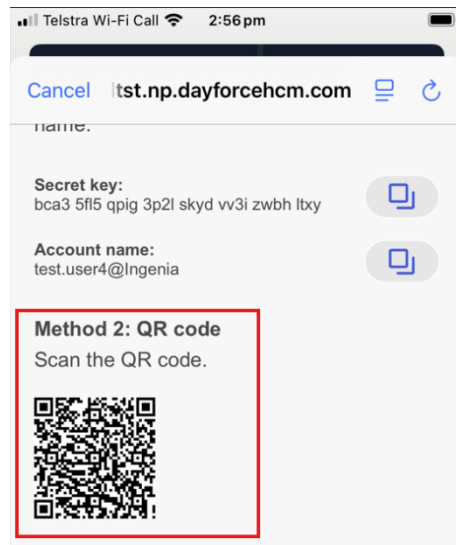
In the **Set up Multifactor Authentication** screen, select **Authenticator App Code** and click **Continue**.



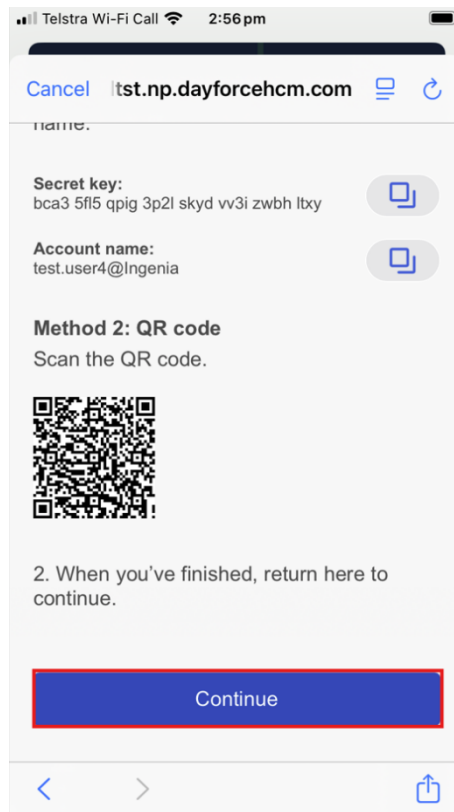
- a. **Method 1: Secret Key and Account:** Manually enter the secret key and account name shown on the screen into your authenticator app.



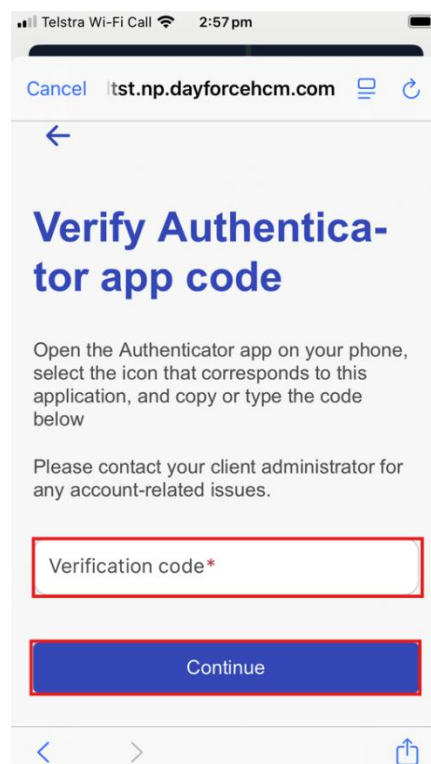
- b. **Method 2: QR Code:** Use your authenticator app to scan the QR code shown on the screen. This will start the process to configure the app with the necessary information.



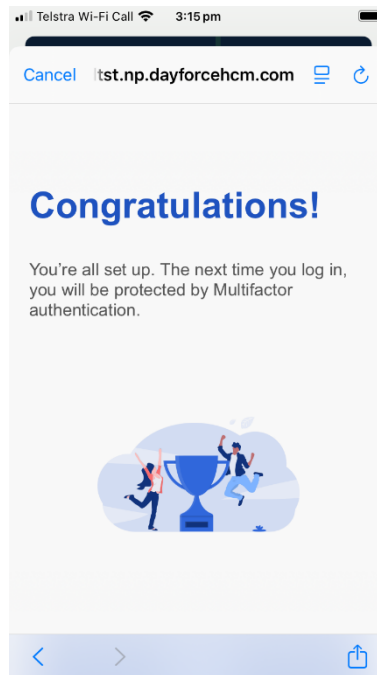
- Once your Dayforce account has been linked to your authenticator app, click **Continue**.



- Open your authenticator app and find the time-based one-time verification code that corresponds with Dayforce. The return to the Dayforce app, and in the **Verify Authenticator app code** screen, enter the verification code. Click **Continue** to log in to Dayforce.

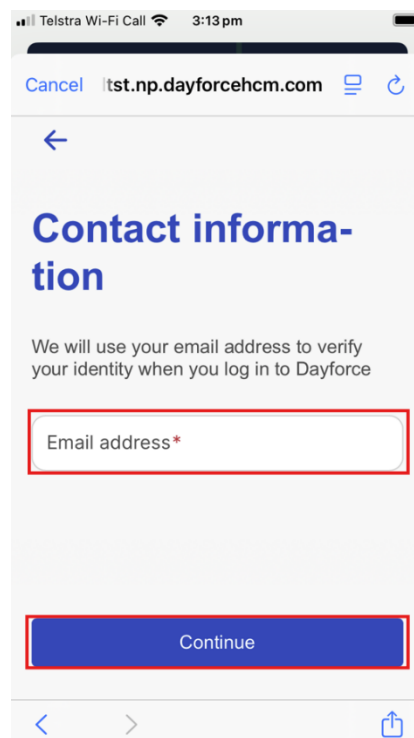


4. Your MFA setup is complete when the completion screen displays.

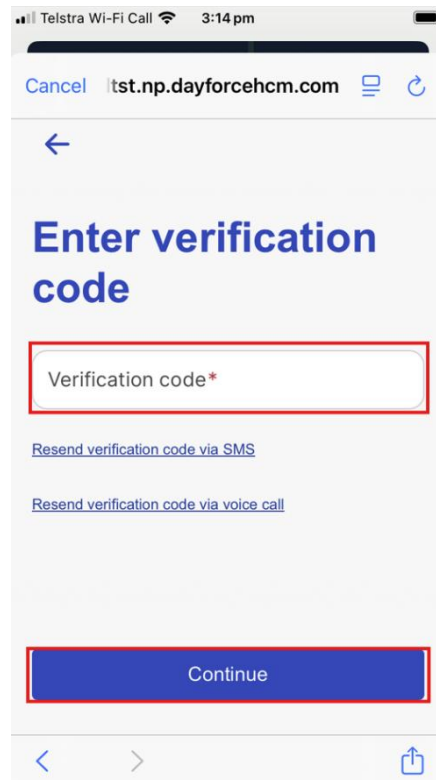


Set Up Multifactor Authentication Using the Email Option

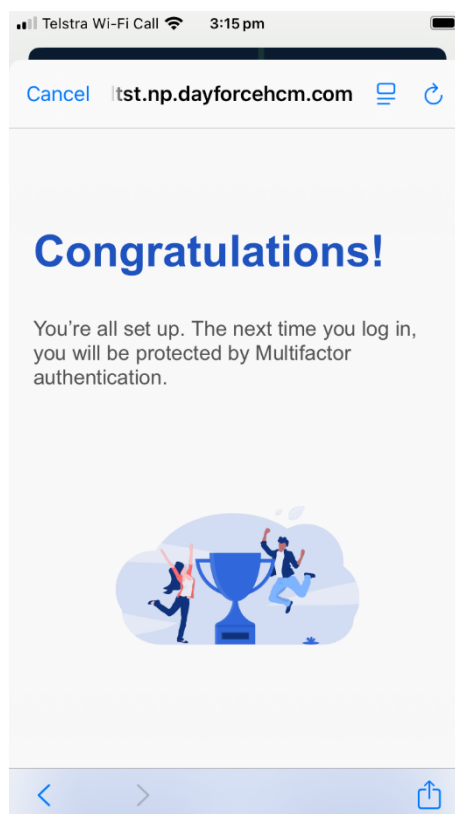
1. After selecting **Email** in the **Set up Multifactor Authentication** screen, you are prompted to set up the authenticator. This option lets you receive time-based one-time verification codes to a valid email address of your choice. In the **Contact Information** screen, enter your email address. Click **Continue**.



2. Open your email and find the time-based one-time verification code from Dayforce. In the **Enter Verification Code** screen, enter the verification code. Click **Continue**.

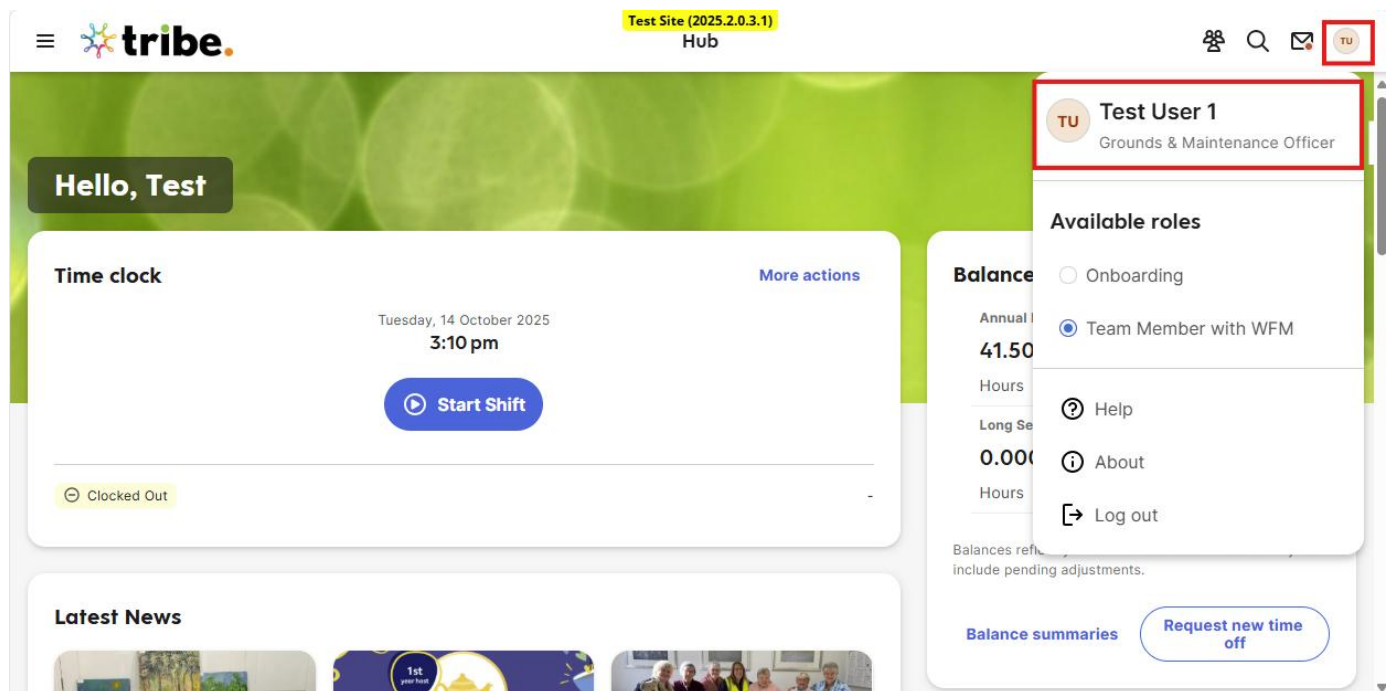


3. Your MFA setup is complete when the completion screen displays.

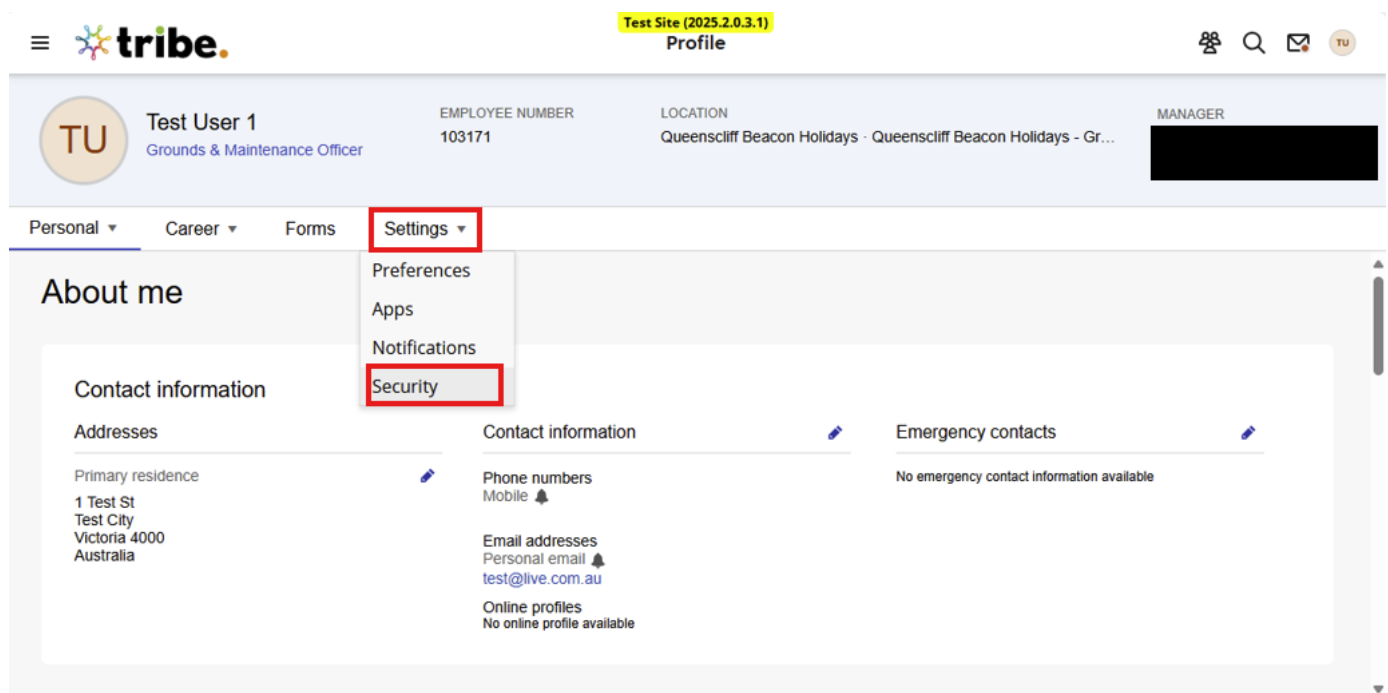


Modifying MFA details

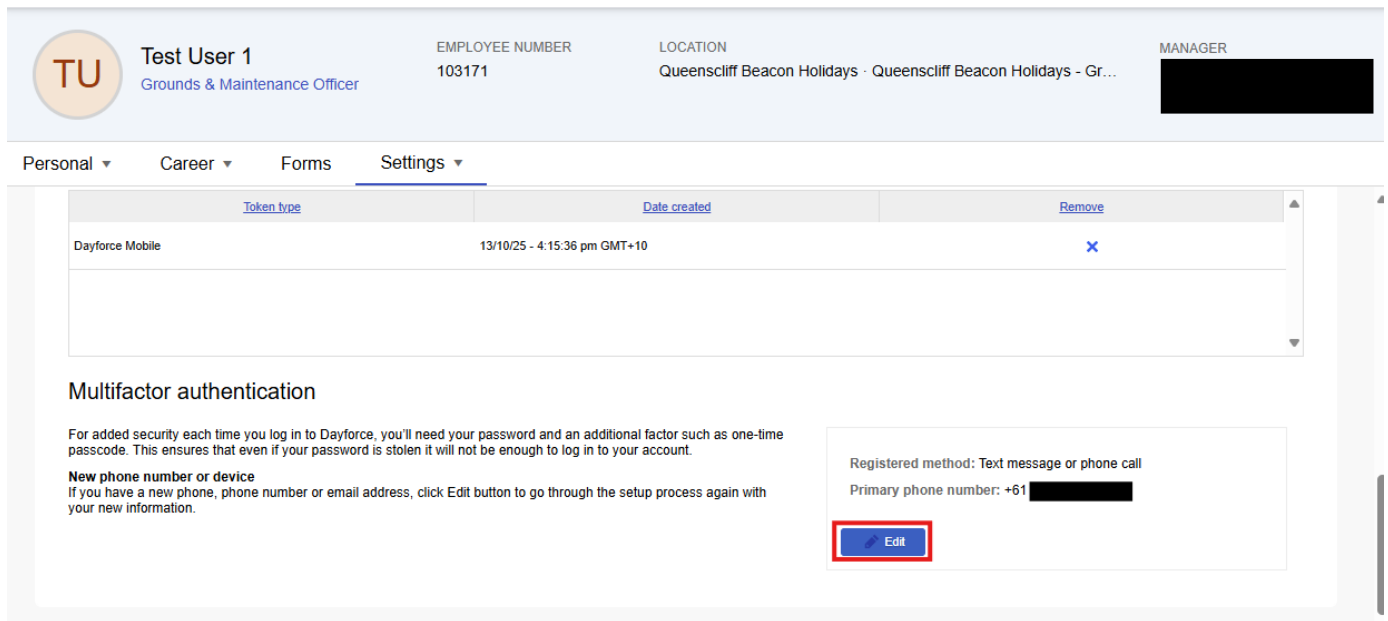
1. Log in on the Tribe Website (not the app) as Team Member with WFM via the following link <https://www.dayforcehcm.com/mydayforce/login.aspx>
2. Navigate to your **profile** by clicking on the circle in the top right corner with your profile picture or two letters, then click on your **name**.



3. Click on **Settings**, then **Security** from the drop down box.

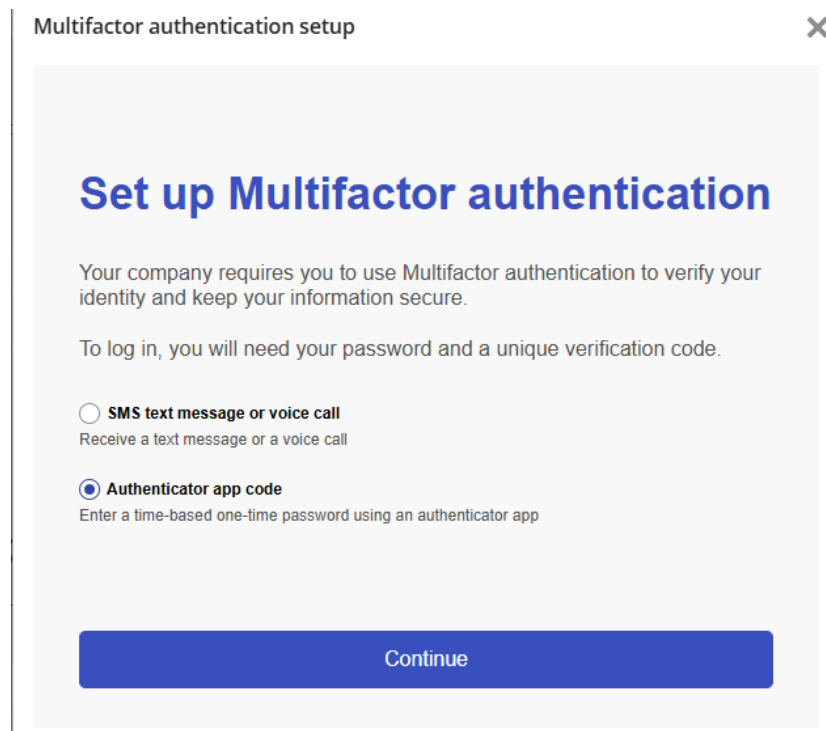


4. Scroll down to the **Multifactor Authentication** section and review the authentication method selected. If this need to change, select the **Edit** button.



The screenshot shows the user profile for 'Test User 1' (Grounds & Maintenance Officer). The 'Settings' tab is selected, and the 'Multifactor authentication' section is visible. It shows a registered method of 'Text message or phone call' with a primary phone number of '+61 [redacted]'. An 'Edit' button is highlighted with a red box.

5. A box will appear giving you the option to set up your MFA method as outlined in the steps in the Setting up MFA – Mobile App section on page 3.



The screenshot shows a 'Multifactor authentication setup' dialog box. It contains the title 'Set up Multifactor authentication' and a message: 'Your company requires you to use Multifactor authentication to verify your identity and keep your information secure. To log in, you will need your password and a unique verification code.' There are two radio button options: 'SMS text message or voice call' (unselected) and 'Authenticator app code' (selected). A 'Continue' button is at the bottom.

For Further Assistance:

If you have any questions or having problems logging into Tribe, please reach out to the People & Culture Team via email to hr@ingeniacommunities.com.au or via phone to 1300 536 518.