astutepayroll

Two Factor Authentication - Employee User Guide

v1.0 Dec 2018

Contents

Overview

What is Two-Factor Authentication?

Two-factor authentication (2FA) is a second level of authentication in addition to a password when a user is accessing their Astute Payroll portal.

The additional authentication is required for all employees when they are accessing their Profile tab, as this includes payroll information such as bank details, tax details and superannuation.

Employees will still be able to access other information in their portal (eg timesheets and expenses) without needing to authenticate.

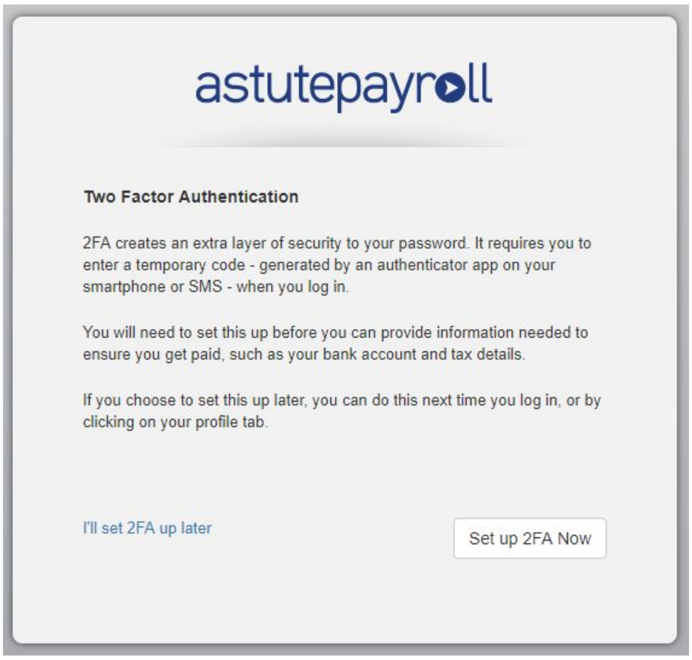
If SMS communications have been configured in a portal, users can choose between receiving an SMS code to a registered mobile number or using a third-party authentication app (Authy or Google Authenticator) to verify their access.

Employees may need to confirm with a portal administrator or their recruiter if they are unsure whether SMS communications are enabled in your portal.

Setting up 2FA as an Employee

When an employee logs into their Astute portal, they will be prompted to set up 2FA if this hasn't already been done.

The employee will be presented with the option to 'Set up 2FA Now' which will start the setup wizard. The employee can also choose 'I'll set up 2FA later' which will redirect them to their portal Dashboard.



Two Factor Authentication

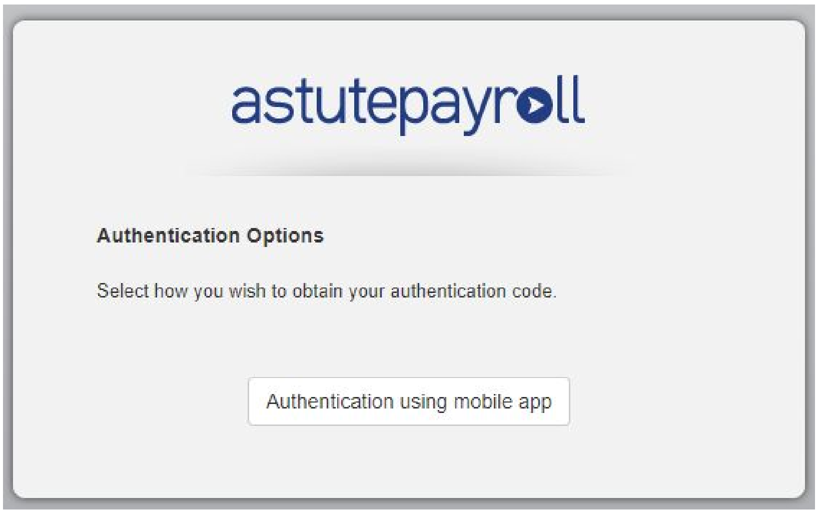
2FA creates an extra layer of security to your password. It requires you to enter a temporary code - generated by an authenticator app on your smartphone or SMS - when you log in.

You will need to set this up before you can provide information needed to ensure you get paid, such as your bank account and tax details.

If you choose to set this up later, you can do this next time you log in, or by clicking on your profile tab.

If the employee clicks ‘Set up 2FA now’, the Authentication Options screen will show the methods that they can choose to set up 2FA.

- ‘Authentication using mobile app option’ will appear for all portals.

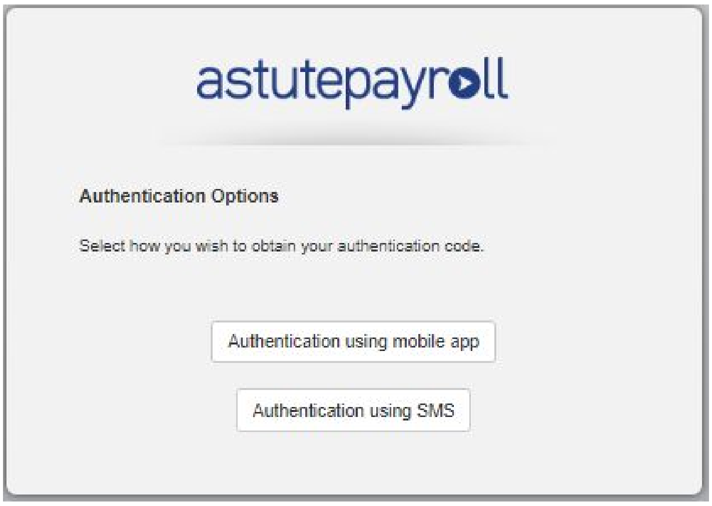


astutepayroll

Authentication Options

Select how you wish to obtain your authentication code.

- ‘Authentication using SMS’ will appear for employees if their portal is enabled with SMS communications. Employees in these portals will be able to select between the two methods.



astutepayroll

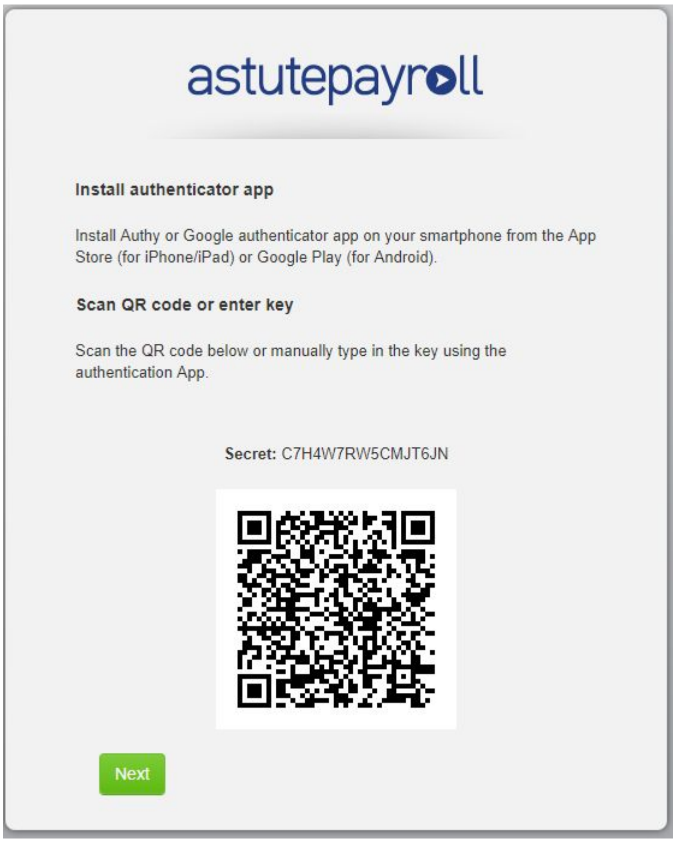
Authentication Options

Select how you wish to obtain your authentication code.

If SMS communications are not enabled for a portal, only the Authentication using mobile app option will appear. This method will need to be used to set up 2FA.

Authentication using a Mobile App

When ‘Authentication using mobile app’ is selected, the Employee will be directed to a screen that includes a QR code and Secret key.



astutepayroll

Install authenticator app

Install Authy or Google authenticator app on your smartphone from the App Store (for iPhone/iPad) or Google Play (for Android).

Scan QR code or enter key

Scan the QR code below or manually type in the key using the authentication App.

Secret: C7H4W7RW5CMJT6JN

Supported Mobile Apps

The authentication process currently supports the Google Authenticator and Authy apps. To proceed with the setup, the user will need to download one of these apps onto their smart phone or device from the App Store (Apple/iOS devices) or Google Play (for Android devices).

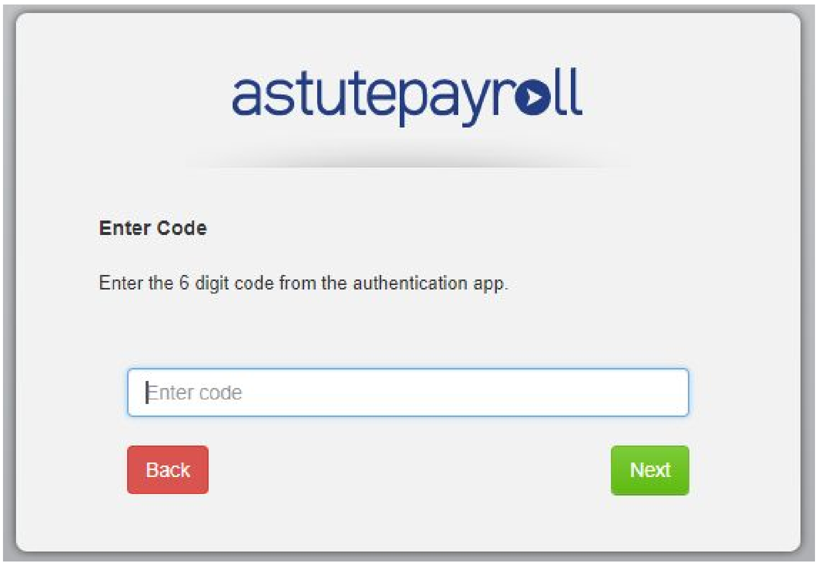
Authenticator Authy

Setup using Mobile App

Once an authenticator app is installed on the user’s smart phone or device, the QR code displayed on the setup screen can be scanned directly to link the device to the user’s Astute portal. Alternatively, the Secret key can be manually typed in.

Click ‘Next’ once the device has been linked to continue with 2FA setup.

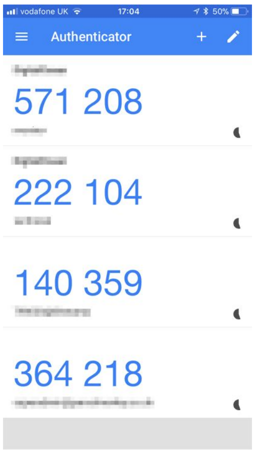
The employee will then be prompted to enter the six digit code from the authenticator app to verify the link.

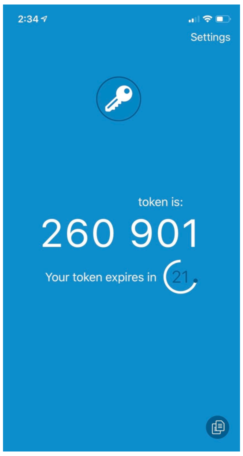


Enter Code

Enter the 6 digit code from the authentication app.

The code in an authenticator app will regularly expire and change after a certain time, so it's important to ensure that the code currently displaying in the app is the code being entered into Astute. An invalid code will be flagged on screen and will need to be re-entered correctly to continue.

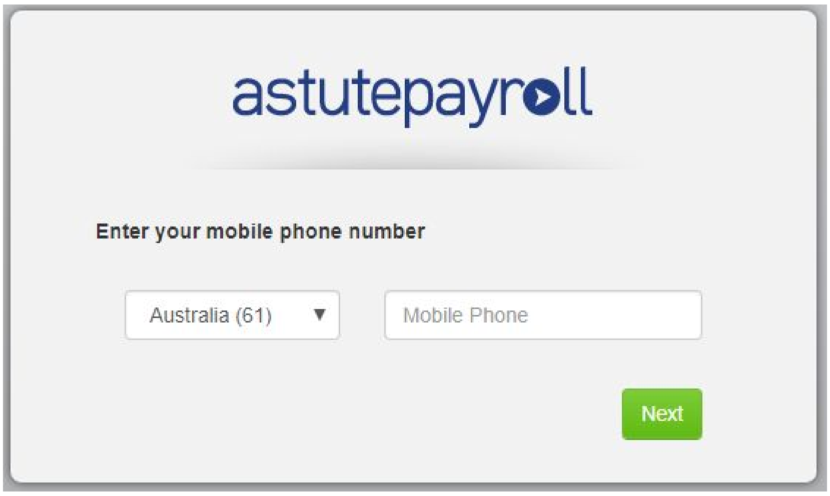




Once the authentication code is entered, click Next to move onto setting up a backup email address. Click Back to return to the previous screen.

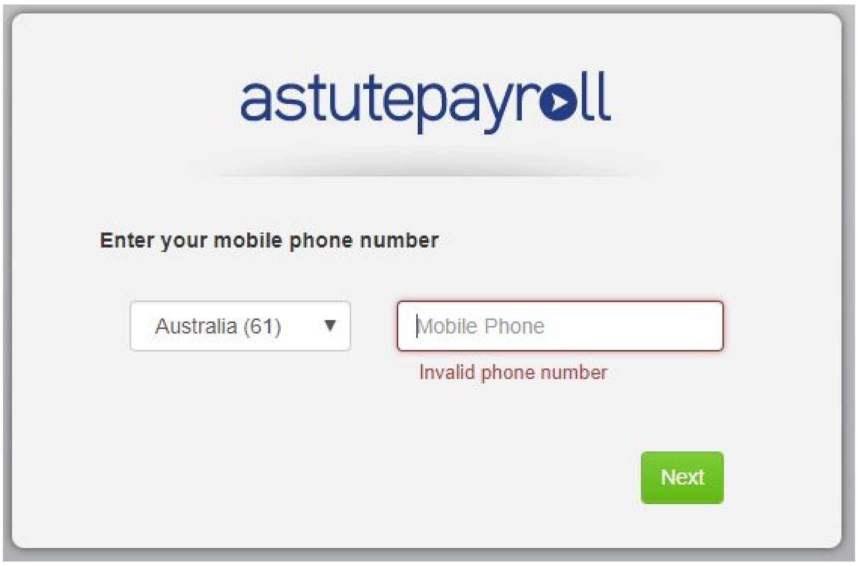
Authentication using SMS

If the option to set up 2FA using SMS is selected, the employee will need to register their mobile number in the field provided then click Next to continue.



Enter your mobile phone number

An invalid phone number will be flagged in red if the format is incorrect (eg invalid characters are entered or the mobile number is incomplete).

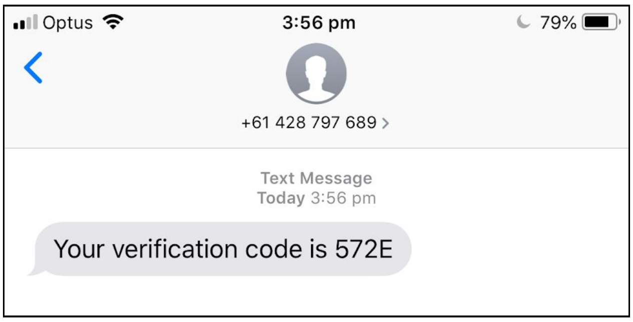


Enter your mobile phone number

Invalid phone number

Please note that the system will only accept Australian mobile numbers. International mobile numbers are not supported. If a user does not have an Australian mobile number, they will need to restart the 2FA setup process and select the authenticator app method instead.

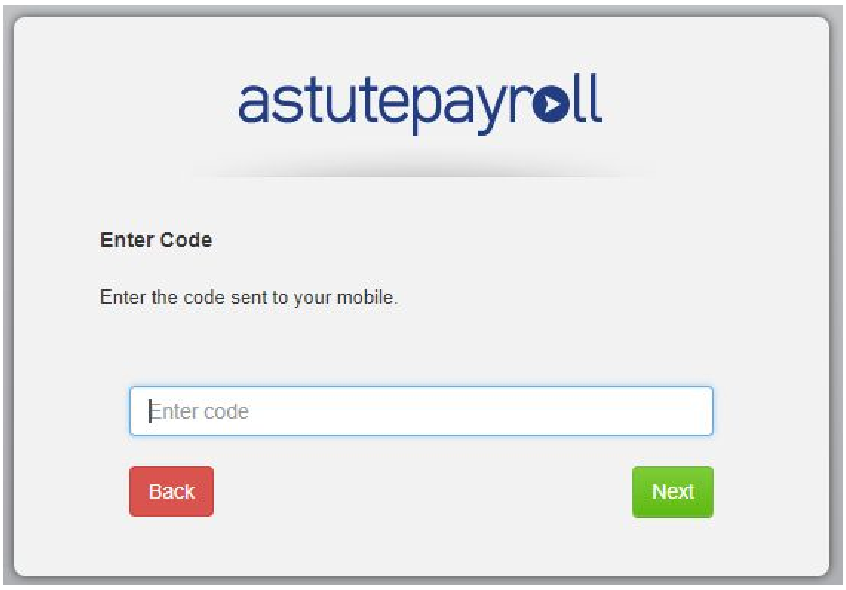
Once the mobile number is entered and validated, an SMS containing a verification code will be sent to the registered number.



Text Message
Today 3:56 pm

Your verification code is 572E

Enter this code to verify the number then click Next to move onto setting up a backup email address.

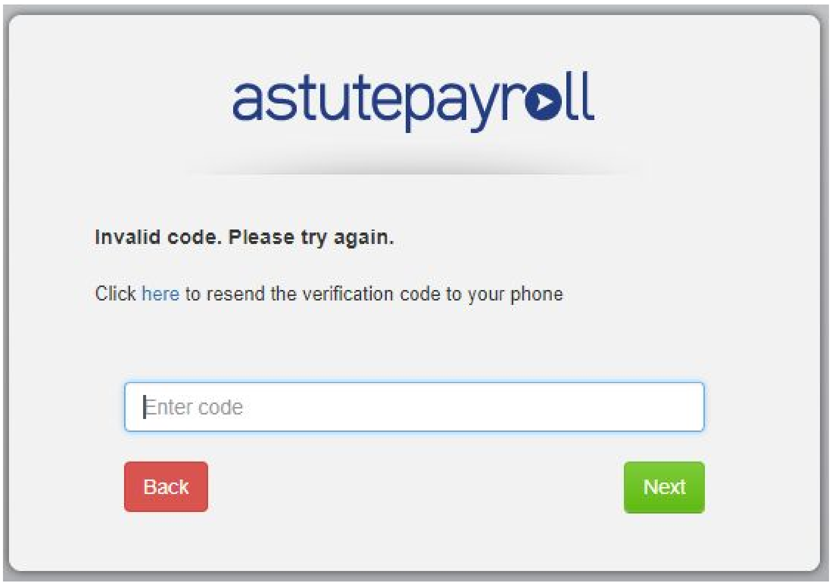


Enter Code

Enter the code sent to your mobile.

If the verification code that is entered is invalid, the administrator will be prompted to re-enter the code. Alternatively, a new SMS code can be generated and sent to the registered number.

Clicking Back will return the employee to the mobile number entry screen.



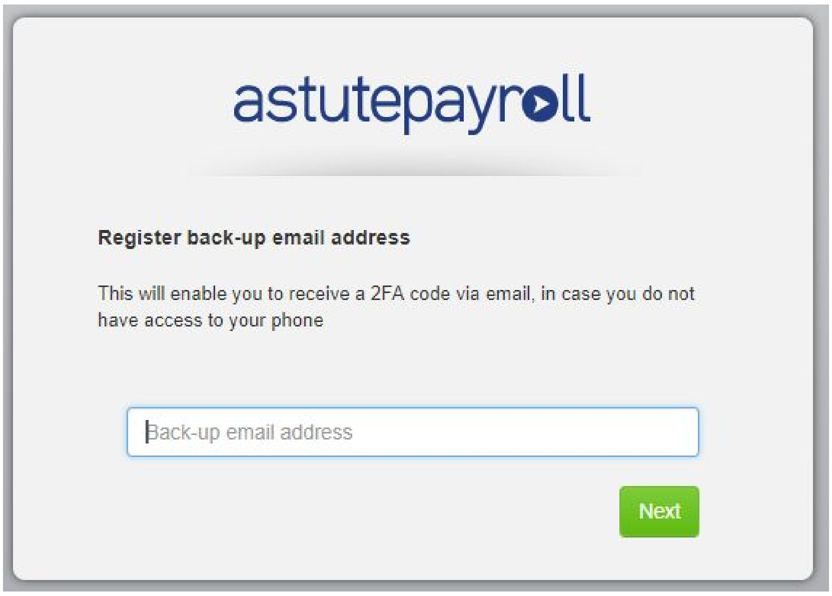
Invalid code. Please try again.

Click here to resend the verification code to your phone

Registering a Backup Email Address for 2FA

The backup email address for 2FA is used when a user is unable to access their usual authentication method.

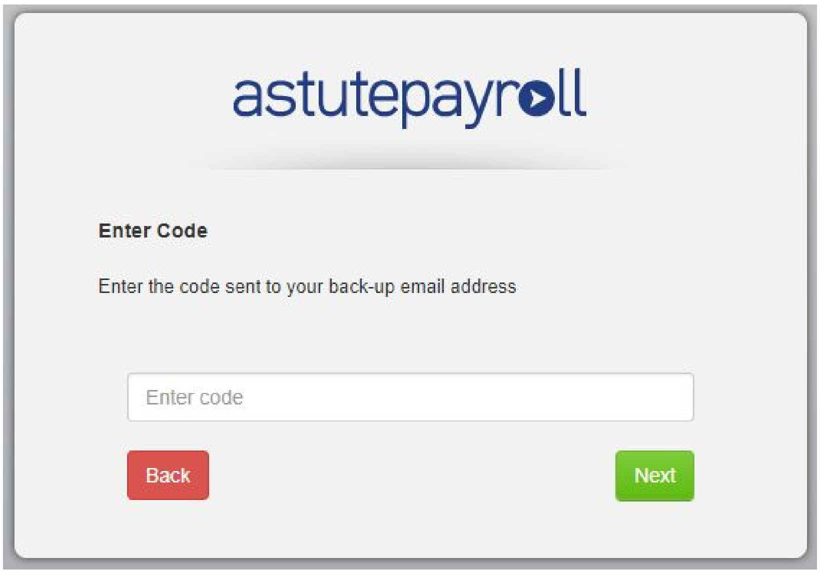
The employee will need to enter their preferred email address and click Next.


astutepayroll

Register back-up email address

This will enable you to receive a 2FA code via email, in case you do not have access to your phone

If the email address is valid, a verification code will be generated and sent to the registered email address. Entering the code from the email notification will verify the backup email address. Click Next to continue.

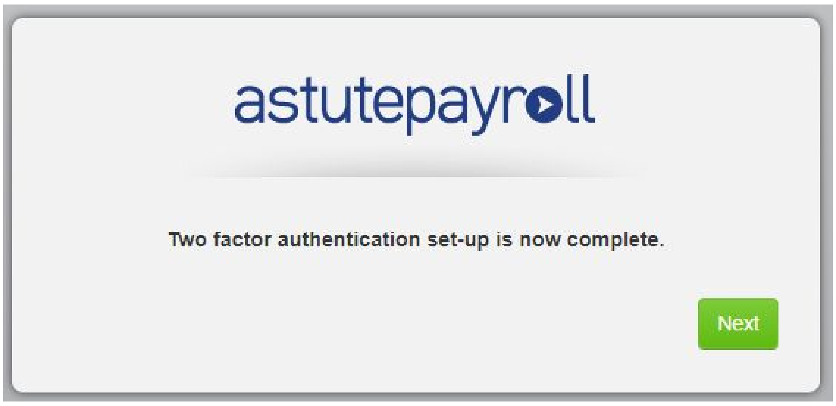

astutepayroll

Enter Code

Enter the code sent to your back-up email address

If the verification code entered is valid, the screen will confirm that 2FA setup is complete.

Clicking ‘Next’ will direct the employee to their Dashboard.



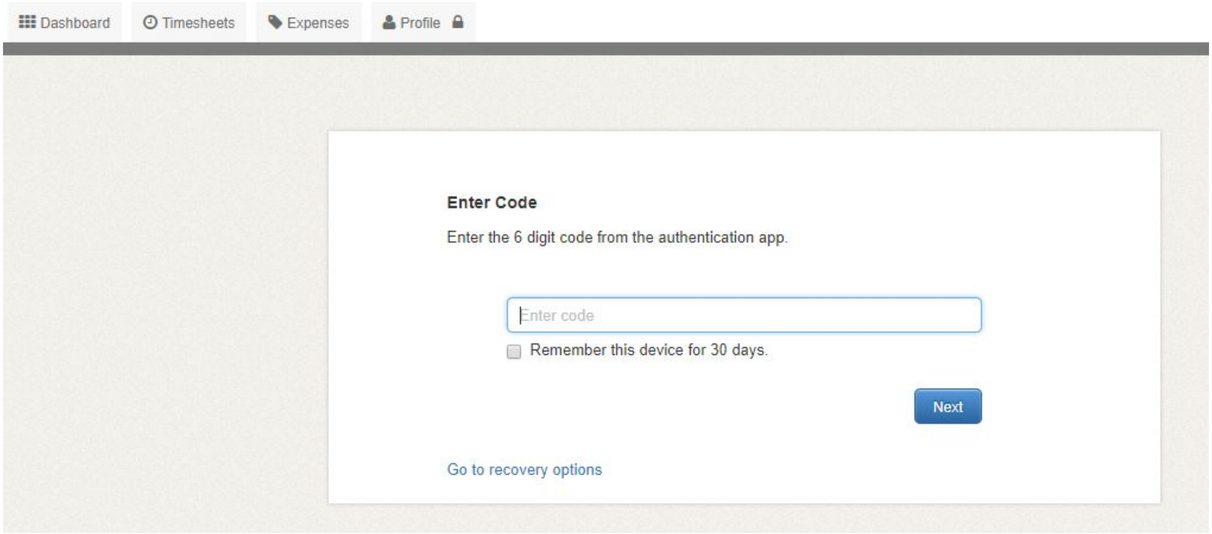
Two factor authentication set-up is now complete.

An invalid code will be flagged on screen and the employee will need to either re-enter the code or request a new code to be sent to their registered backup email address.

Accessing your Profile tab using 2FA

An employee will be prompted to verify using 2FA when they access the Profile tab in their portal.

If 2FA has been set up via an app, enter the six digit code from the authentication app and click Authenticate.

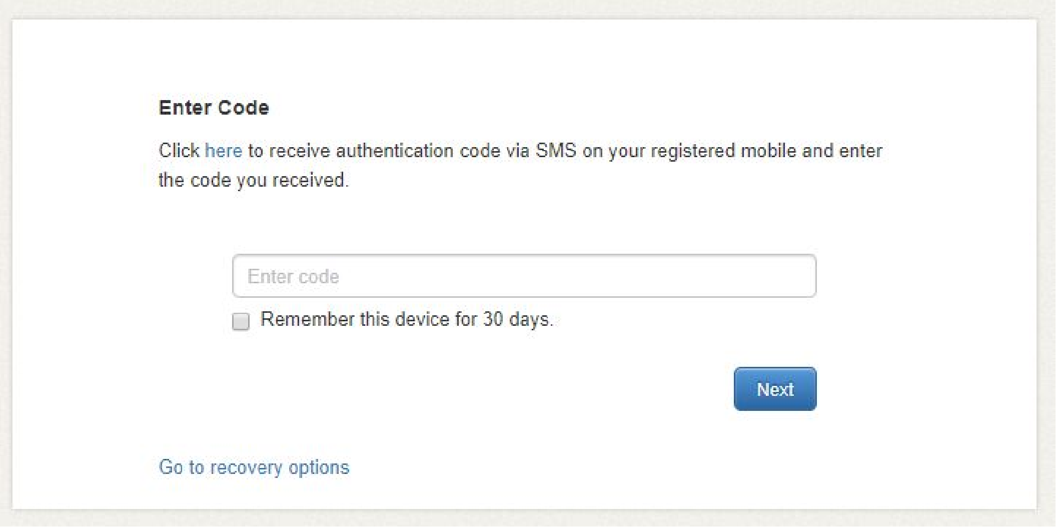


Enter Code

Enter the 6 digit code from the authentication app.

□ Remember this device for 30 days.

If SMS authentication is being used, the employee can trigger an SMS code to be sent to their registered mobile number by clicking ‘here’ (as per screenshot below). Once the SMS code is received, enter this in the verification screen and click Authenticate.

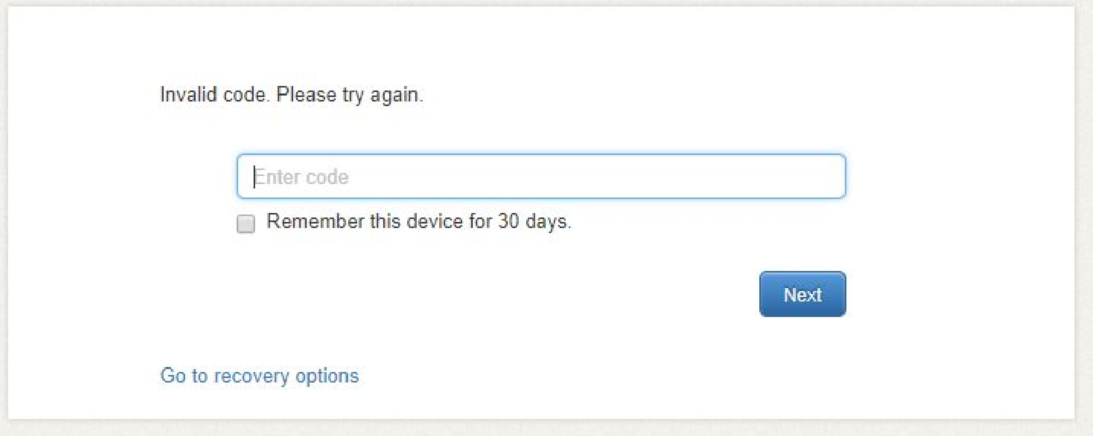


Enter Code

Click here to receive authentication code via SMS on your registered mobile and enter the code you received.

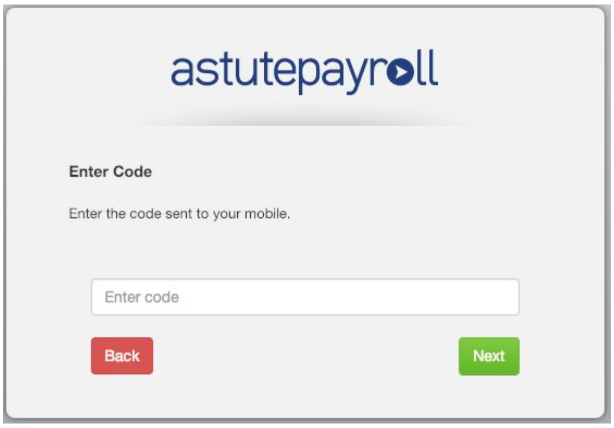
Upon successful authentication, the employee will be granted access to their Profile tab.

If the verification from the authentication app fails (eg the code is entered incorrectly), the employee will be prompted to try again. Employees using an app will need to enter the code that is currently displaying on their device as this is the active code.



Invalid code. Please try again.

If the verification from the SMS code fails, employees can nominate to have a new code sent to their mobile by clicking ‘Back’.



Enter Code

Enter the code sent to your mobile.

Remembering a Device

Employees can tick the 'Remember this device for 30 days' checkbox and will not be required to re-authenticate their access from that device for the following 30 days.

This means that when they log into their portal and click to access their Profile tab on a verified device during this period, they will be able to view their personal information without authentication.

After the 30 days has passed, the employee will need to re-authenticate themselves the next time that they access their Profile tab.

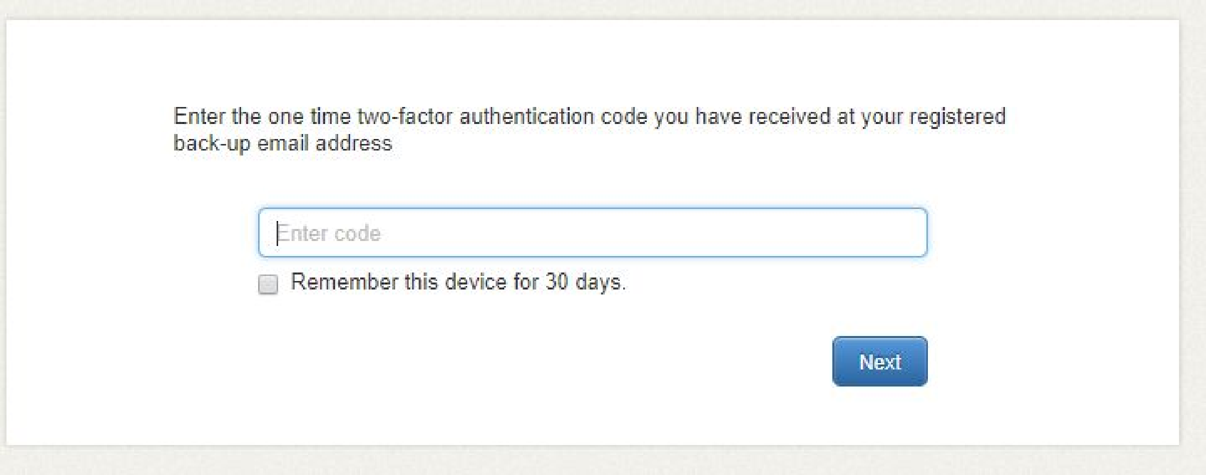
If the 'Remember this device for 30 days' checkbox is not ticked, the employee will be prompted to authenticate each time they access their Profile tab.

Using the Backup Email Address to Authenticate

If an employee is temporarily unable to access the device that they have linked to 2FA, they can use their backup email address to receive a verification code.

From the 2FA verification screen:

1. Click Recovery Options > No access to 2FA device temporarily. This will prompt an email notification to be sent through containing a one-time authentication code.
2. Type the code into the 'Enter code' field.
3. Click Next.



Enter the one time two-factor authentication code you have received at your registered back-up email address

If the code is valid, the employee will be able to access their Profile tab. If the verification fails, the employee will need to re-enter the code or request a new authentication code to be emailed.

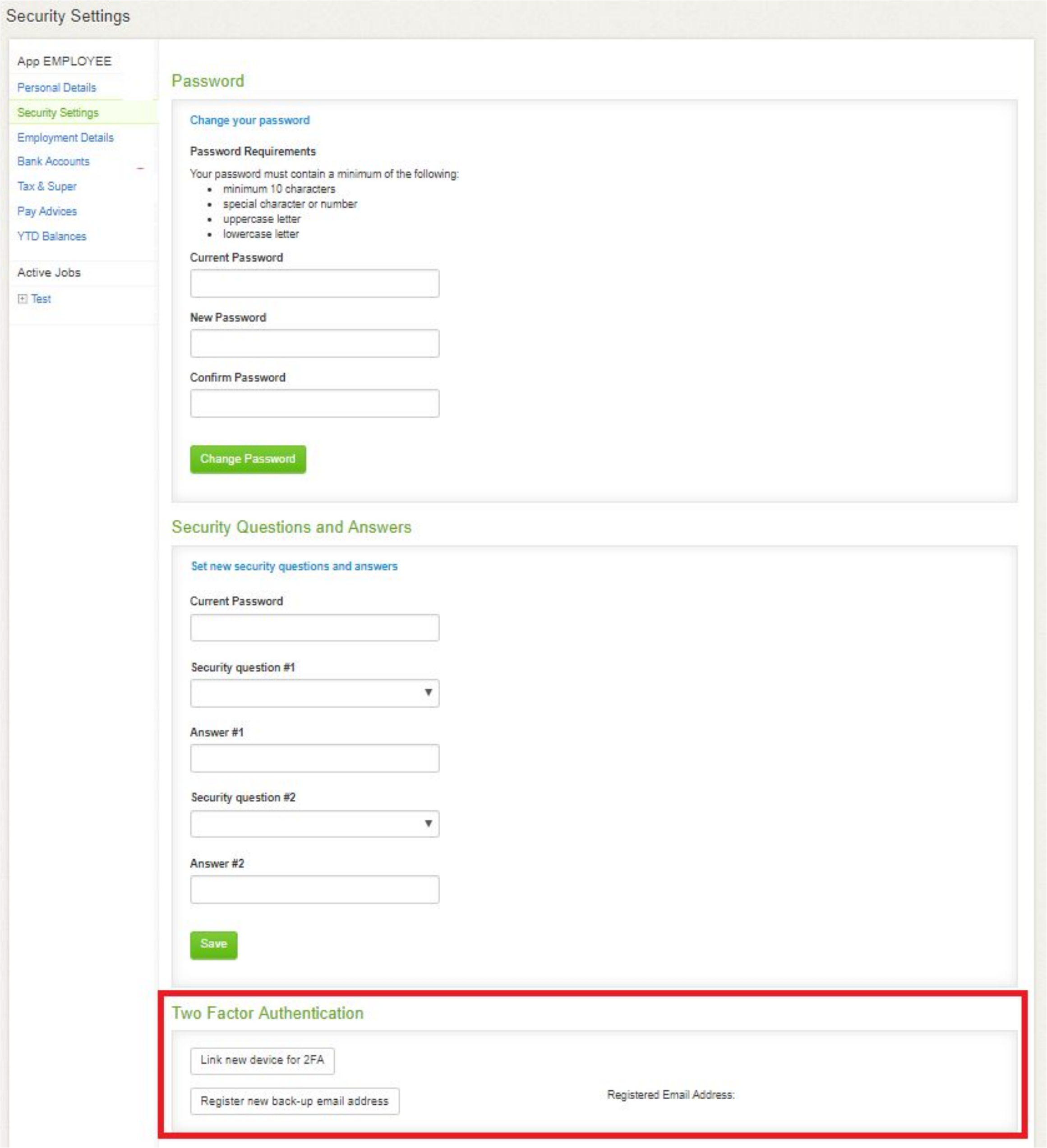
Forgotten Password and Backup Email Address

If a user is not able to access their backup email address or doesn't know which email address they have set up, they will need to contact a Portal Administrator to have their 2FA settings reset.

Managing 2FA Settings in your Profile

The details that are registered for 2FA can be managed by an employee from the Profile > Security Settings screen. Depending on how 2FA has been configured for the user, there are a number of options that will appear.

Link new device for 2FA	Change the smartphone/device to verify a user with an authentication app. This option will only appear for users who verify via an authentication app.
Change phone number registered for 2FA	Change the mobile phone number that is currently being used to receive the authentication codes. This option will only appear for users who verify via SMS.
Register new back-up email address	Change the email address that is linked to 2FA for the user. This option will appear for all users regardless of the verification method they have set.



Your password must contain a minimum of the following:

- minimum 10 characters
- special character or number
- uppercase letter
- lowercase letter

Linking a new device for 2FA

To link a new device to an employee, the current device will first need to be verified.

1. Go to the Profile tab > Security Settings > Link new device for 2FA.
2. Enter the six digit code from the authentication app on your current device and click Next.
3. Scan the QR code that displays using the camera of the new device or enter the Secret key manually into the app.
4. Enter the six digit code from the authentication app on the new device and click Next to verify the link.

Once the code is verified, a confirmation will appear on screen that the new device has been successfully linked and the employee can proceed to their Profile tab.

Register a new backup email address

To update the backup email address registered for an employee:

1. Go to your Profile tab > Security Settings > Register new back-up email address. This will prompt a notification to be sent to the current backup email address.
2. Enter the code from the email into the empty field and click Next.
3. Enter the current email address and the new email address, then click Next. If both email addresses are valid and correctly formatted, the employee will be advised that the email address has been successfully updated.
4. Click ‘Continue to access the portal’.

Register a new mobile number for 2FA

The mobile number linked to 2FA for an employee can be updated from the 2FA verification screen by following the steps below.

1. Go to Recovery Options > Change phone number registered for 2FA.
2. Enter the SMS verification code sent to the current phone number, then click Next.
3. Enter the Current mobile phone number and the New mobile phone number, ensuring that they are formatted correctly and include the Australian prefix (+61).
4. Enter the SMS verification code sent to the new mobile number and click Next.

Once the new mobile number is verified, future verification codes will be sent to this number.

The system will advise that the mobile number has been updated. Clicking ‘Continue to access the portal’ will return the employee to their portal Dashboard.