

MFA

Multi-Factor Authentication

Employer Access/ Online Portal
and SCH Online User Guide



Contents page

Multi-Factor Authentication

What's New?	3
What do I need to do?	3
First set up of existing EmployerAccess/Online and SCH Online users	4
Okta Verify	5
Google Authenticator	6
New contact created by existing user	7
Regular sign on	8
Okta Verify	8
Google Authenticator	9
Reset Multi-Factor Authentication	10
Unable to Login to EmployerAccess/Online	10
How do I create a user in EmployerAccess/Online and SCH Online?	11

Multi-Factor Authentication

What's New?

In April 2021 we will be making changes to the way users sign in to EmployerAccess/Online and SCH Online platform. These changes are being developed to protect your data and comply with the ATO's Operational Framework, a multi-factor authentication sign-in process will soon be added to the Rest login page.

You will still be able to sign in using the same email address/username and password, but in addition you will need to provide an additional security check upon signing in by providing either a code sent to your nominated device or a push notification.

What do I need to do?

In preparation for Multi-Factor Authentication you need to ensure that you have updated your information on your Rest EmployerAccess platform. Review your existing contact list and ensure your contact list is up to date; you have set up a unique login for each user that is transacting on behalf of your business.

Did you know you have the ability to add multiple contacts on your account? If you are not sure how to do this

Upon selecting your preferred method of authentication, you will be required to download the Rest application on either your mobile phone or tablet. This is simply to complete the additional level of authentication. You will not be able to see any employer details and personal information will not be recorded on this device.

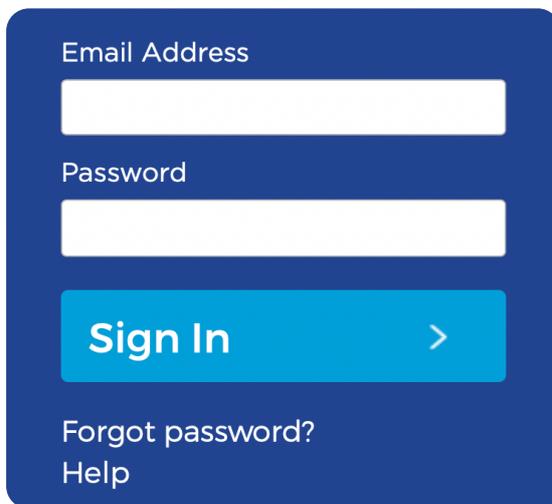
First set up of existing EmployerAccess/Online and SCH Online users

01

'Sign In' through the portal to begin the process.

If you currently have an EmployerAccess/Online and SCH Online account - signing in will be easy. Simply navigate to the Rest website and 'Login' through the portal to begin the process.

[Click here to log in to Rest EmployerAccess](#)

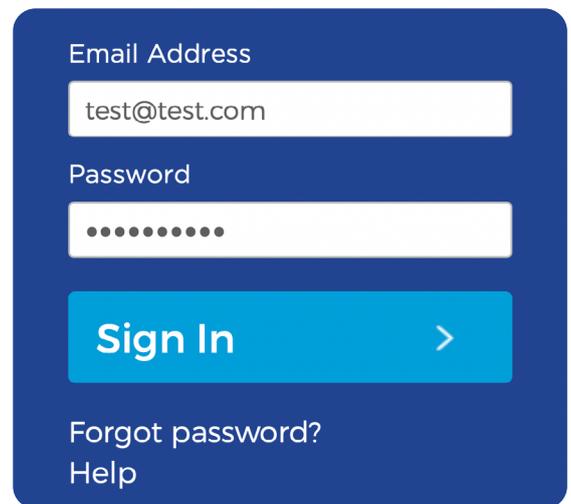


The screenshot shows a dark blue login form with two white input fields. The first field is labeled 'Email Address' and the second is labeled 'Password'. Below the fields is a blue button with the text 'Sign In' and a right-pointing chevron. At the bottom left, there are two links: 'Forgot password?' and 'Help'.

02

Enter your email address/username

and password on this screen and select 'Sign In' to continue.



The screenshot shows the same login form as in step 01, but with the 'Email Address' field containing 'test@test.com' and the 'Password' field filled with ten black dots. The 'Sign In' button and links are still visible at the bottom.

03

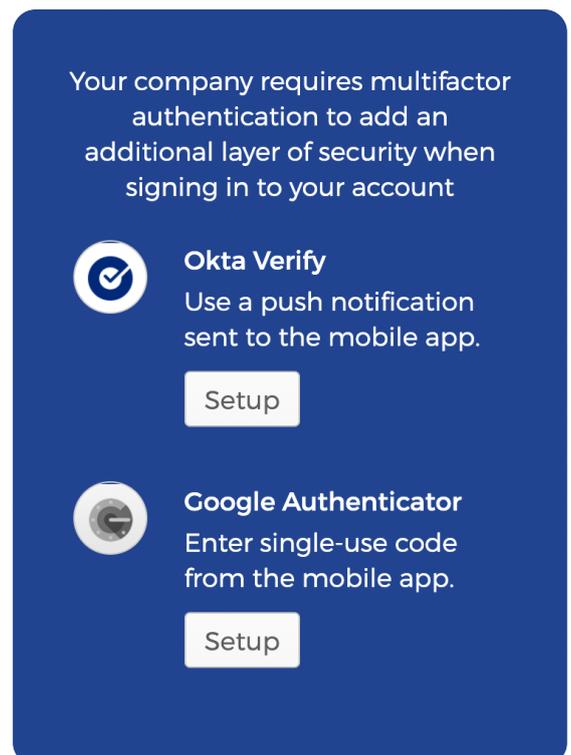
After successful 'Sign In' the below prompt will appear to set up your Multi-Factor Authentication.

You will be asked to choose between 'Okta Verify' or 'Google Authenticator'.

'Okta Verify' will allow you to choose either a push notification or a manual code trigger that will appear on the device you downloaded the application on.

'Google Authenticator' will trigger a single-use code on the device you downloaded the application on.

You must select one.



The screenshot shows a dark blue screen with the heading 'Your company requires multifactor authentication to add an additional layer of security when signing in to your account'. There are two options, each with a circular icon and a 'Setup' button. The first option is 'Okta Verify' with a checkmark icon, described as 'Use a push notification sent to the mobile app.' The second option is 'Google Authenticator' with a 'G' icon, described as 'Enter single-use code from the mobile app.'

Okta Verify

Select your device type

If you have selected Okta Verify as your preferred method of authentication you will be asked to select what device you will be downloading the application on.

'Select your device type' from the options above or go to your preferred application store to download the application.

Once you have downloaded the Okta Verify application on your device you will need to launch the application and select 'Add an account'.

Proceed to **'Scan barcode'**.

Select your device type

iPhone

Android

[Back to factor list](#)

Launch Okta Verify application on your mobile device and select Add an account.



Can't scan?

[Back to factor list](#)

Can't Scan?

If you can't scan the barcode select 'Can't scan?', this will give you a link that you will need to follow in order to set up Okta Verify.

You can configure any additional optional factor or click finish

Enrolled factors

Okta Verify

Additional optional factors

Google Authenticator
Enter single-use code from the mobile app.

[Setup](#)

[Finish >](#)

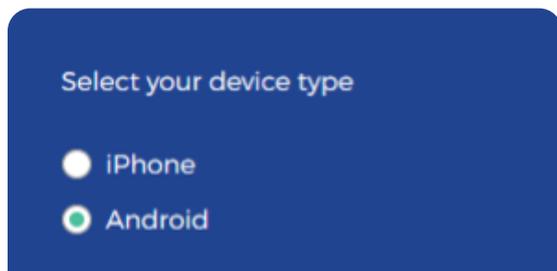


Select 'Finish' this will complete your set-up.

After the first time setup is complete, you will be signed in to EmployerAccess/Online dashboard.

Google Authenticator

If you have selected Okta Verify as your preferred method of authentication you will be asked to select what device you will be downloading the application on.

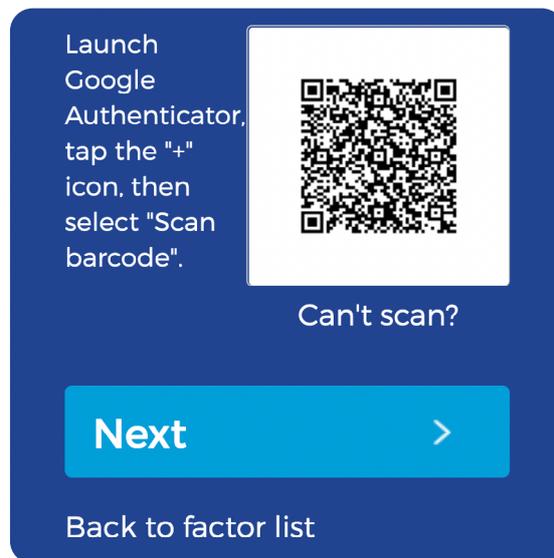


'Select your device type' from the options above or go to your preferred app store to download the application.

Once you have downloaded the Google Authenticator application on your device you will need to launch the application and select **'Add an account'**.

Proceed to:

'Scan barcode' and select 'Next'.



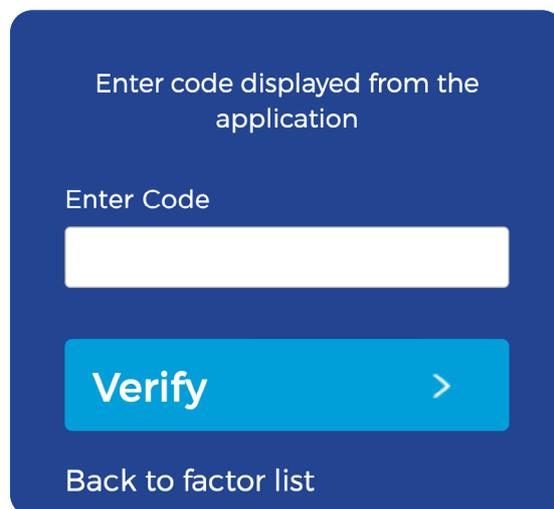
Can't Scan?

If you can't scan the barcode select 'Can't scan?', this will give you a link that you will need to follow in order to set up Okta Verify.

You will be required to enter the 6 digit verification code that will appear on the Google Authenticator application and select 'Verify'.

This will complete your set-up.

After the first time setup is complete, you will be signed in to EmployerAccess/Online dashboard.



New contact created by existing user

01

New Rest users will go through a similar process as existing users who are signing in for the first time. The entire flow has been documented here to illustrate this process.

Communication was sent to your employer to ensure that all users are created within EmployerAccess/Online with a unique account and linked to the respective employer accounts.

Upon being set up for access to EmployerAccess/Online by your company, a registration email will be sent to your inbox with your login credentials.

This should include your username and password.

Activate Okta Account

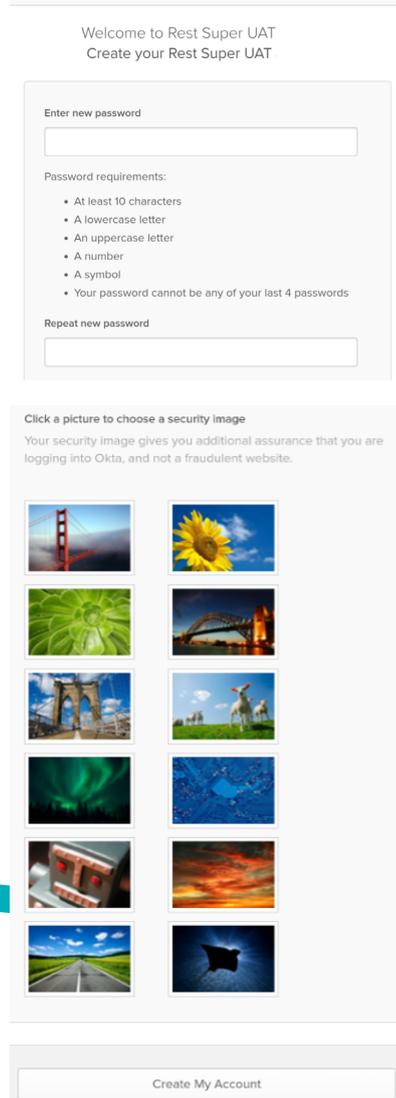
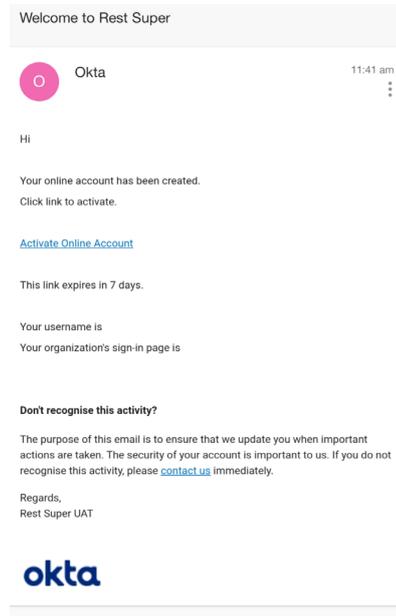
02

When you proceed to the 'Activate Okta Account' link you will be prompted to create a password.

Create My Account

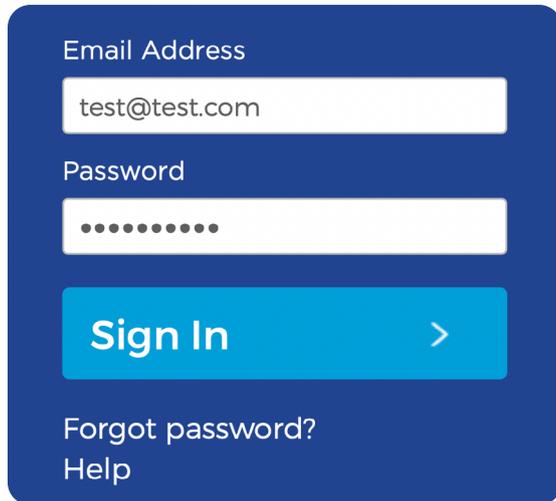
03

Once you have chosen a password, security image and selected 'Create My Account' you will be prompted to set up Multi-Factor Authentication.



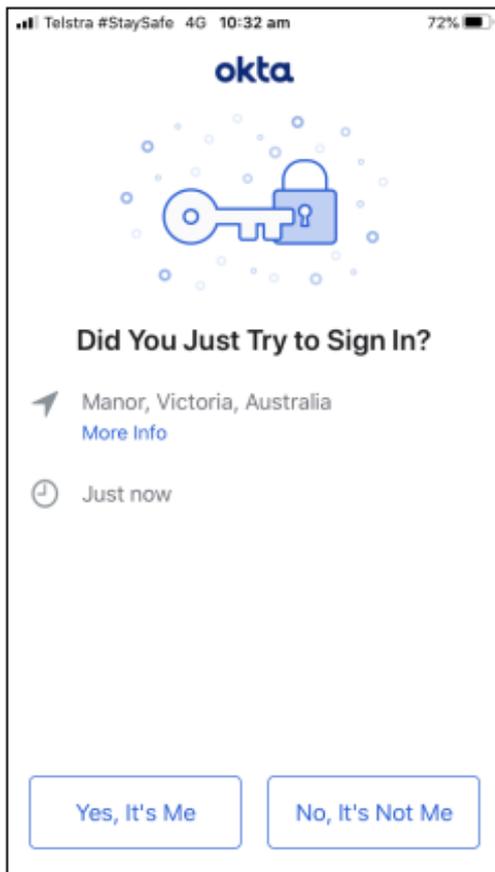
Regular Sign On

Enter your email address/username and password then select, 'Login' to continue.



A dark blue sign-in form with white text and input fields. It contains an 'Email Address' field with 'test@test.com', a 'Password' field with masked characters, a blue 'Sign In' button with a right-pointing chevron, and links for 'Forgot password?' and 'Help'.

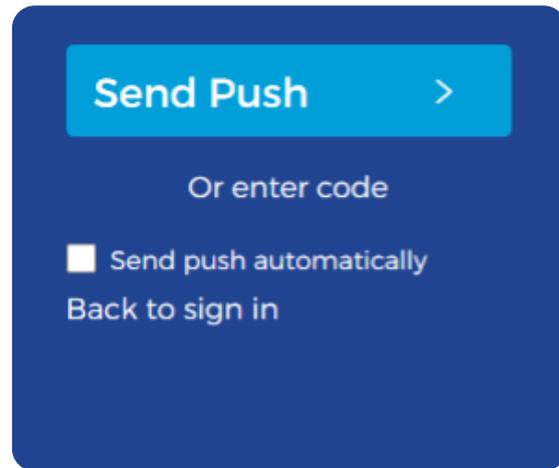
If you have selected '**Send Push**', you will see the below image on the Okta application you have downloaded to your device.



Okta Verify

If you have set up Okta Verify you will see the following screen, you will be given the option to;

- 1) 'Send Push' notification to your phone or
- 2) 'enter code' manually.
- 3) 'Send push automatically'.



A dark blue screen for Okta Verify. It features a large blue button labeled 'Send Push' with a right-pointing chevron. Below this is the text 'Or enter code'. There is a checkbox labeled 'Send push automatically' which is currently unchecked. At the bottom is a link that says 'Back to sign in'.

Select, '**Yes, it's me**' to proceed and verify your additional level authentication.

You can also select to 'Send the push automatically' by ticking the box as shown above.

What if it's not me?

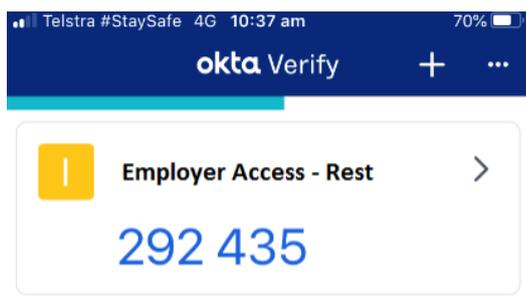
If you have received this notification on your Okta application and you have not attempted to login to EmployerAccess/Online select, 'No, it's not me'.

You can check within your internal organisation if someone has attempted to transact using your login credentials. You need to ensure that your company has created a unique login for anyone that needs to transact on this account through EmployerAccess/Online immediately as they will not be able to login EmployerAccess/Online with Multi-Factor Authentication. Please proceed to

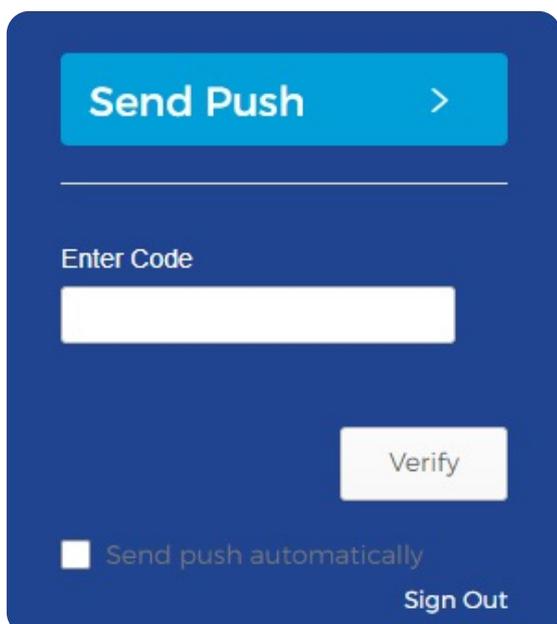
; for assistance.

Alternatively, please contact us and one of our friendly operators will be able to assist you.

If you have selected the 'enter code' as an option, you will receive a code on the Okta application you have downloaded to your device.



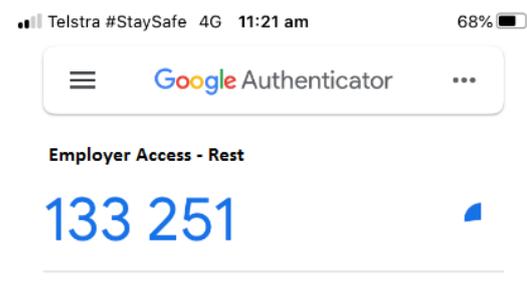
Enter the code and select, 'Verify'. You will be signed in to EmployerAccess/Online dashboard.



Google Authenticator

If you have set up Google Authenticator you will receive a 6 digit code to the application you have downloaded on your device.

Enter the 6 digit validation code in the field as shown below and select, 'Verify'.

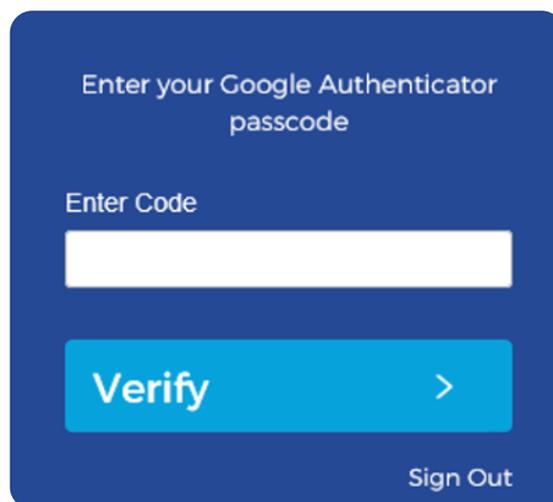


You will be signed in to EmployerAccess/Online dashboard.

What if the code does not work?

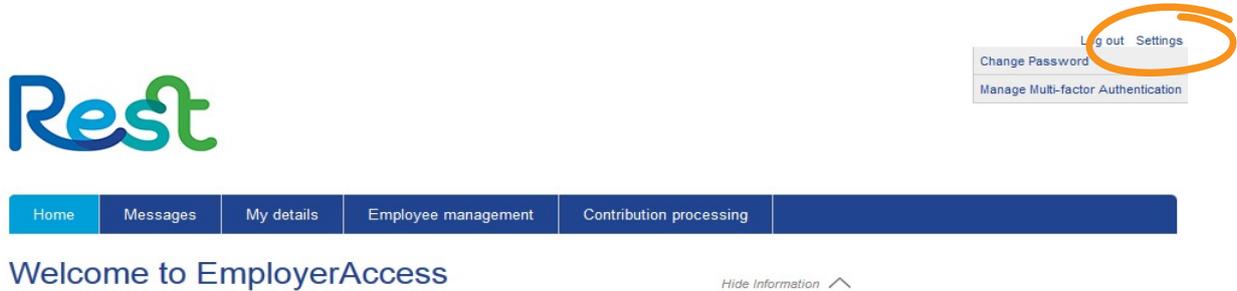
Verify that you are attempting to use the correct account, alternatively trigger another code and try again.

If you are still having issues logging in please contact us and one of our friendly operators will be able to assist you.

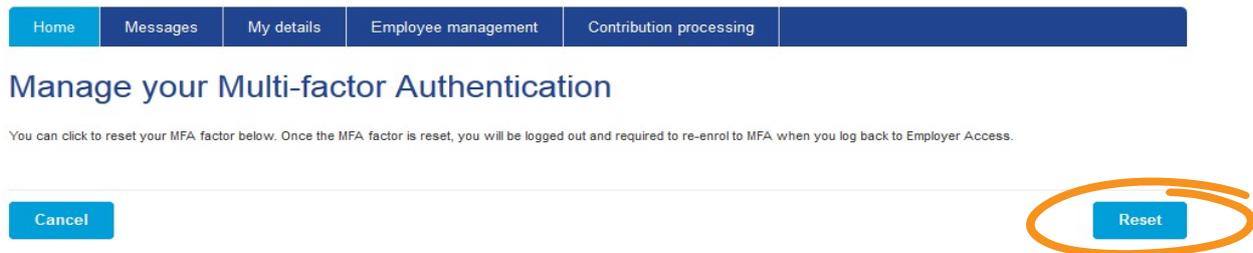


Reset Multi-Factor Authentication

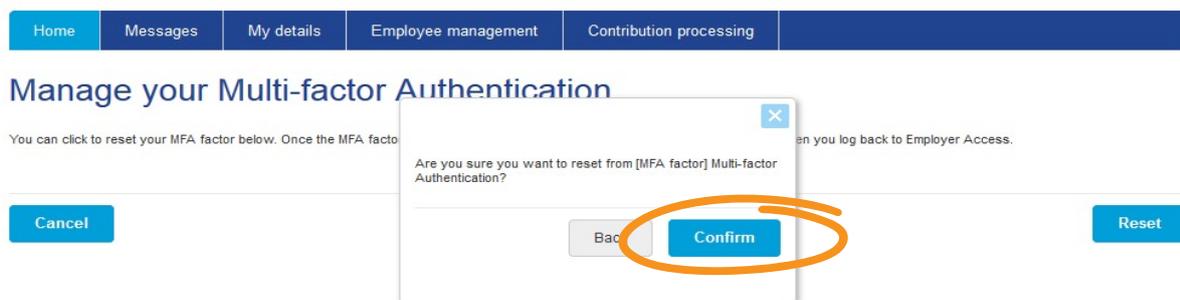
You can reset your Multi-Factor Authentication at any time; below we have outlined how you can do this. Once you have logged in to your EmployerAccess/Online account, select **'Settings'** in the top right corner of the screen and then select 'Manage Multi-Factor Authentication'.



The below screen will appear, select the **'Reset'** button.



A pop up will appear asking you to **'Confirm'** this action.

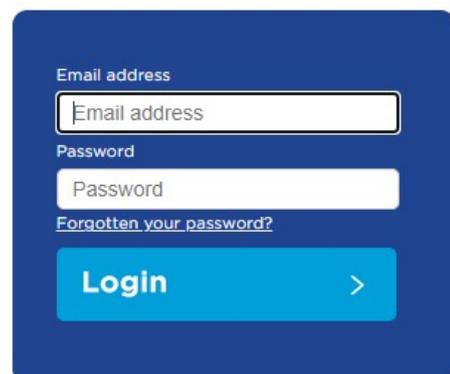


You will be automatically signed out of EmployerAccess/Online and returned to your [Rest login page](#). Proceed to setting up your Multi-Factor Authentication again as shown in the steps

Unable to Login to EmployerAccess/Online

If you are unable to log in please use the 'Forgotten your password?' function via the log in page to reset your password. This can be found on the login page.

If you are still unable to reset your password through the login page please use the **'Contact Us'** feature, or call our contact centre at 1300 305 775 during 8am to 8pm AEST/AEDT and one of our friendly operators will be able to assist you.



How do I create a user in Employer Access/Online and SCH Online?

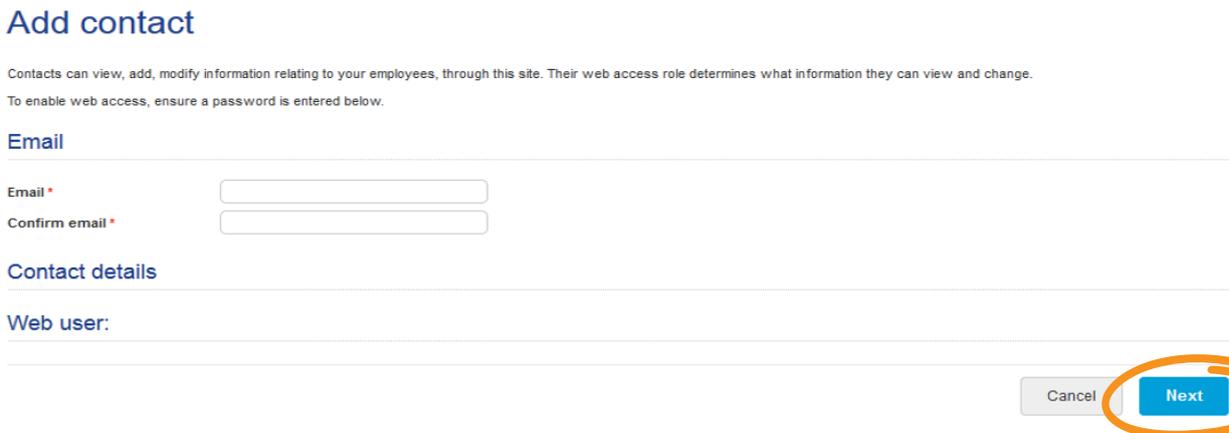
In your employer online portal navigate to the 'My Details' tab, select **'Manage contacts'**



The below screen will appear, select **'Add Contact'**



Enter the new contacts email address and select **'Next'**.



The below screen will appear.

Here you will need to provide all details in the fields marked with an * as these are mandatory fields.

Select the 'Web role' for the contact you are adding.

The user role you have assigned to the contact will determine the level of access and visibility they will have on this account.

When you have filled out all mandatory fields, select '**Create contact**'.

The contact will now receive an email with their login credentials.

Email

Email *	<input type="text" value="test@company.com"/>
Confirm email *	<input type="text" value="test@company.com"/>

Contact details

Title *	<input type="text" value="Mr"/>	Country *	<input type="text" value="AUSTRALIA"/>
Position *	<input type="text" value="Employer Contact"/>	Address line 1 *	<input type="text" value="1 Test Street"/>
First name *	<input type="text" value="John"/>	Address line 2	<input type="text"/>
Last name *	<input type="text" value="Citizen"/>	Suburb *	<input type="text" value="Test Suburb"/>
Phone *	<input type="text" value="0200000000"/>	Postcode *	<input type="text" value="2000"/>
Mobile	<input type="text"/>	State *	<input type="text" value="New South Wales"/>

Web user:

Web role *	<input type="text"/>
Primary Contact	<input type="radio"/> Yes <input checked="" type="radio"/> No



We're here to help

 rest.com.au

 [Live Chat at rest.com.au](#)

Monday to Friday 8am – 10pm and Saturday 9am – 6pm AEST

 **1300 305 775**

Monday to Friday 8am – 8pm