Southern Cross Health Insurance

Welcome

New Provider Web multi-factor authentication (MFA) user guide

Thank you for taking the time to read over these guidelines and partnering with us to create a seamless experience for our members.

If you require any further assistance, please give us a call on:
0800 757 838 or email us at aps@southerncross.co.nz

Southern Cross Health Insurance

Provider Web multi-factor authentication (MFA) user guide

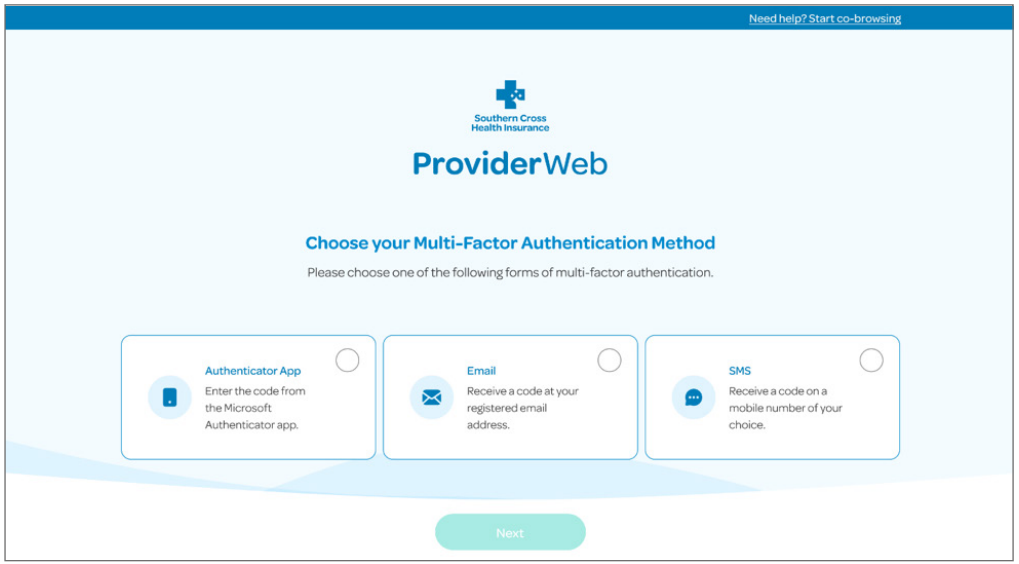
March 2025

Contents

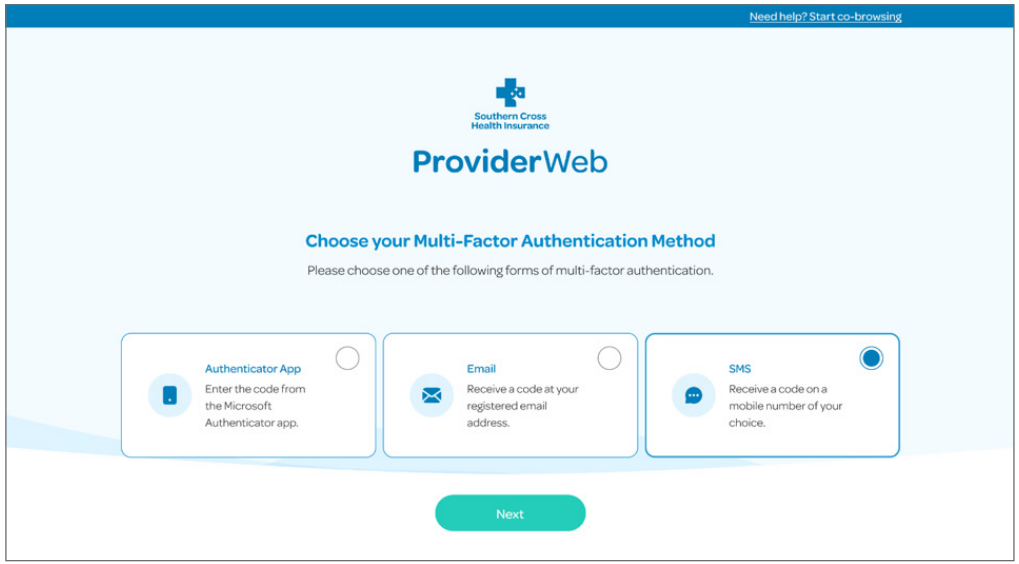
Selecting your MFA method	4
Authenticator app flow	5
SMS (text) flow	10
Email flow	13
Setting up MFA when you don’t know your password	17
We’re here to help	21

Selecting your MFA method

Make your way to Provider Web and you will be presented with these options.

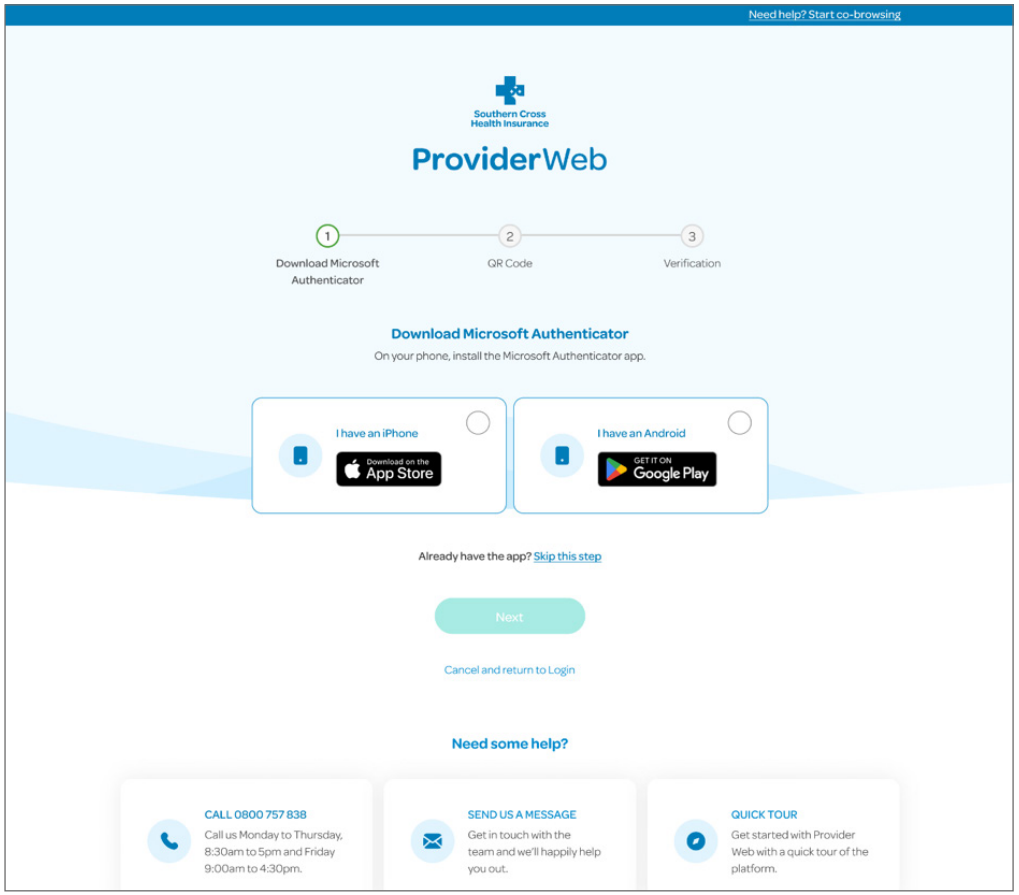


Select your preferred method and you will then be directed to the appropriate flow.

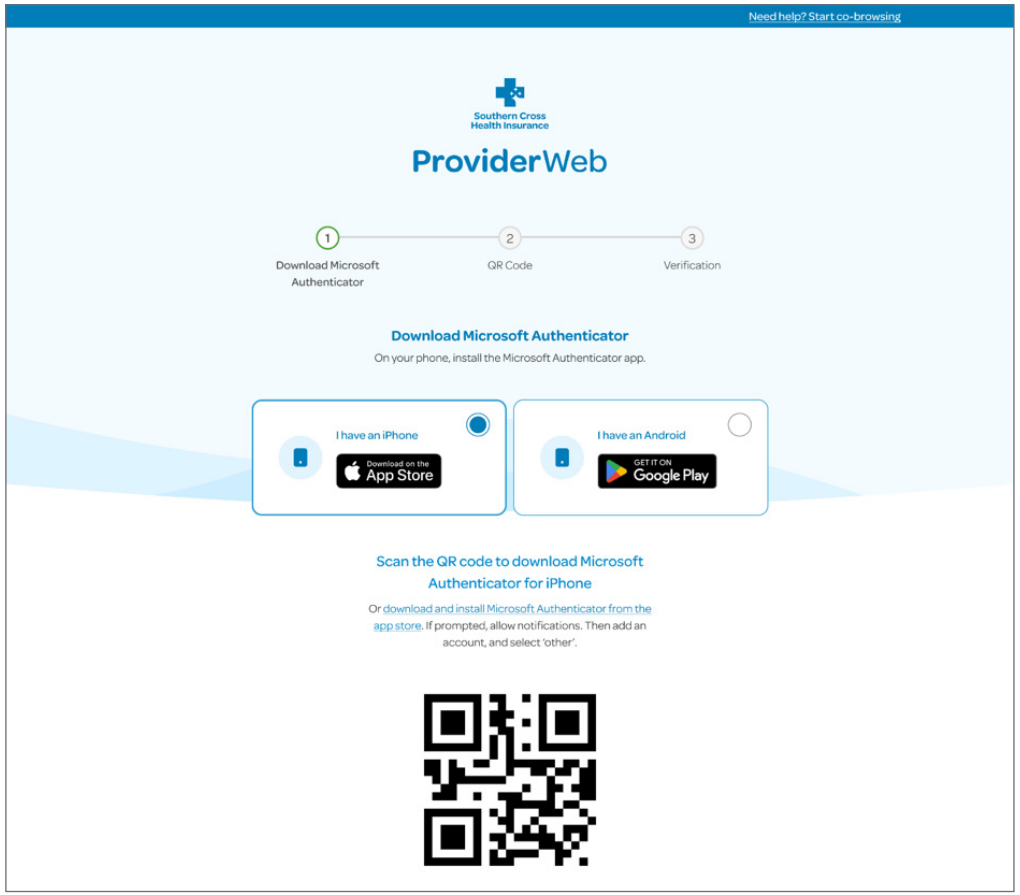


Authenticator app flow

Below is the flow you will follow if you choose authenticator app as your preferred MFA method.

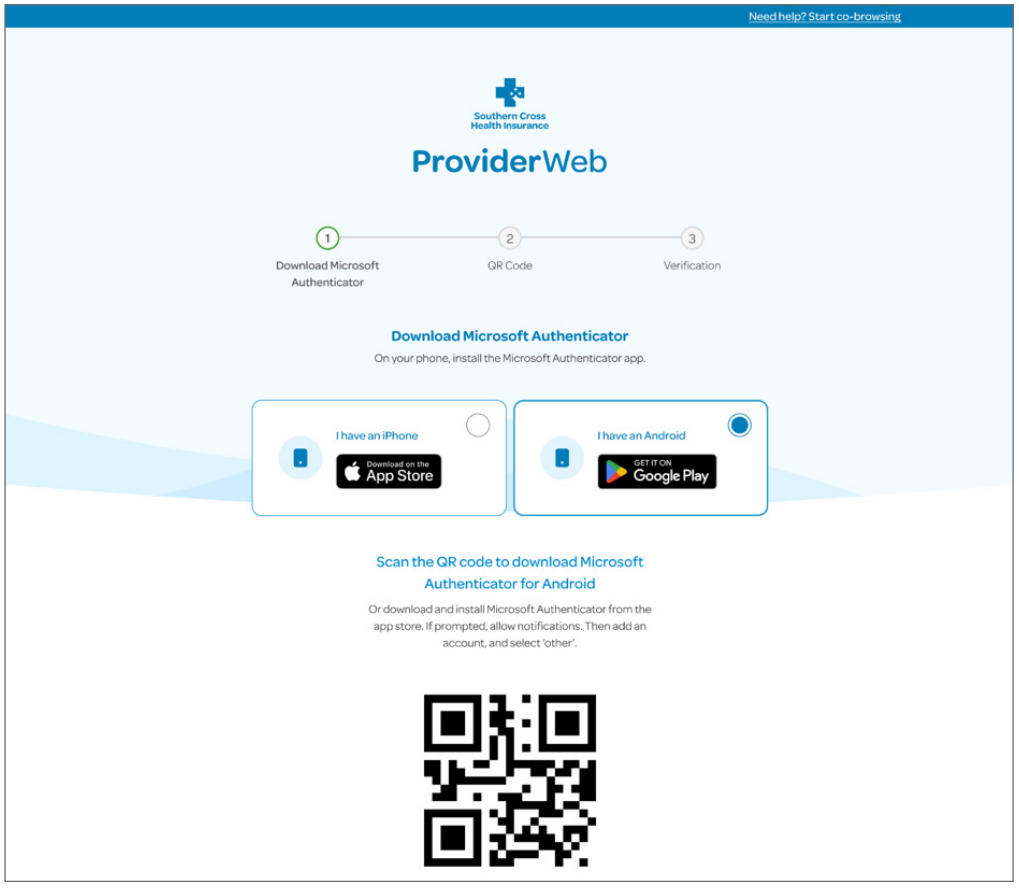


If you have an iPhone select the **'I have an iPhone'** option.

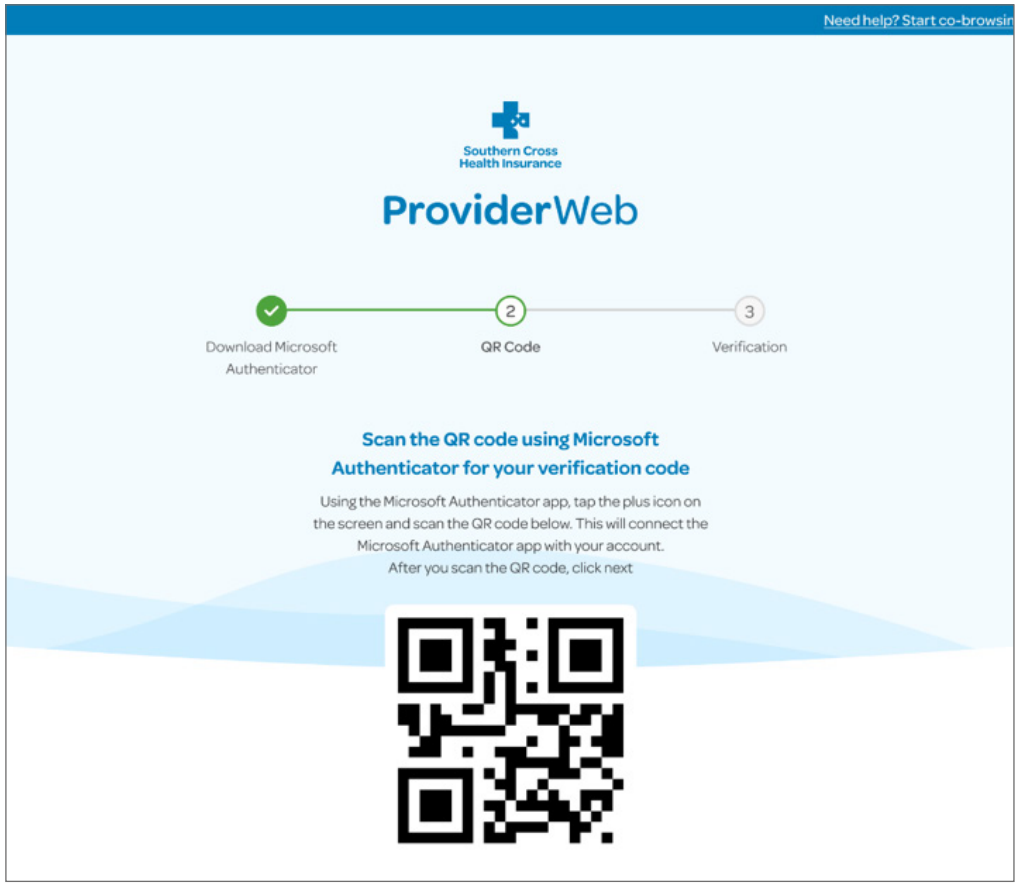


Authenticator app flow

If you have an Android device, select the **'I have an Android'** option.

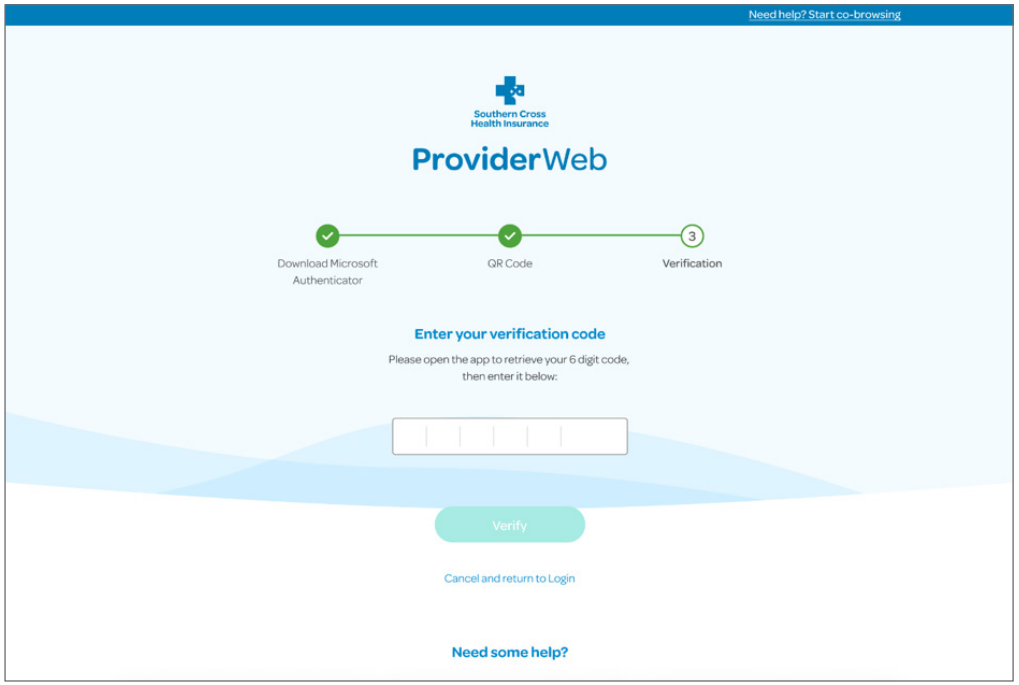


You will then be redirected to scan the QR code.

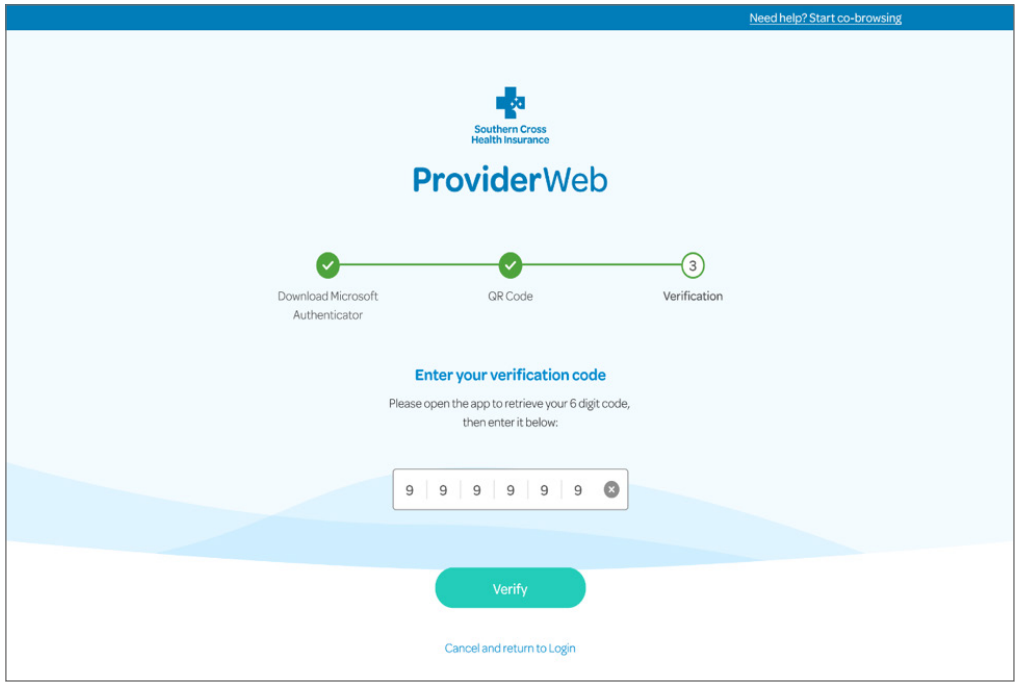


Authenticator app flow

Enter the verification code that will pop up on the authenticator app on your phone.

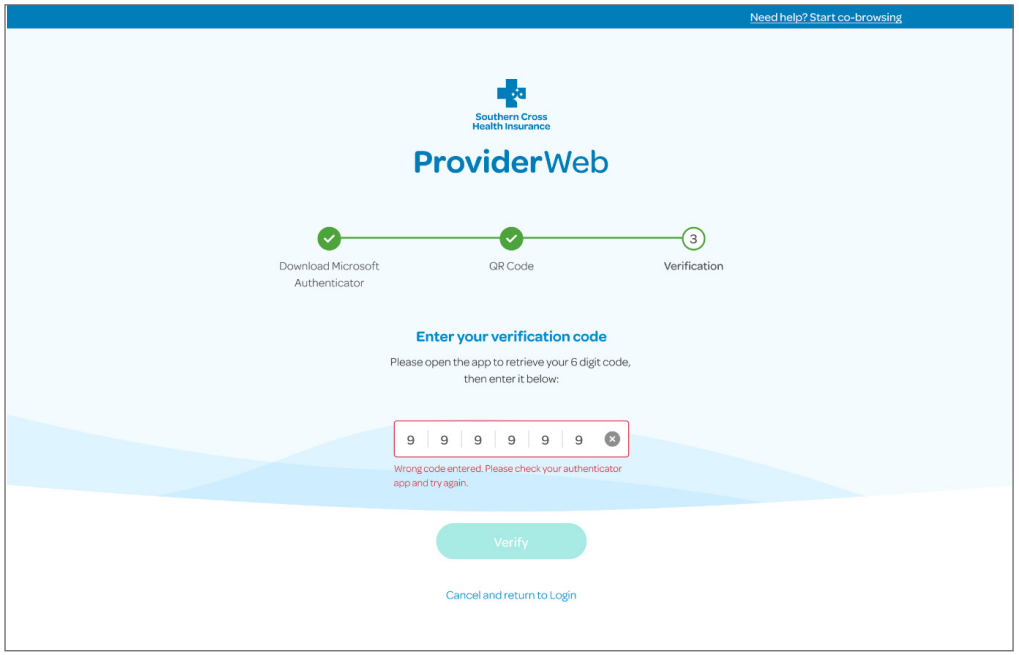


The green **'verify'** box will become clickable after you enter the correct code.

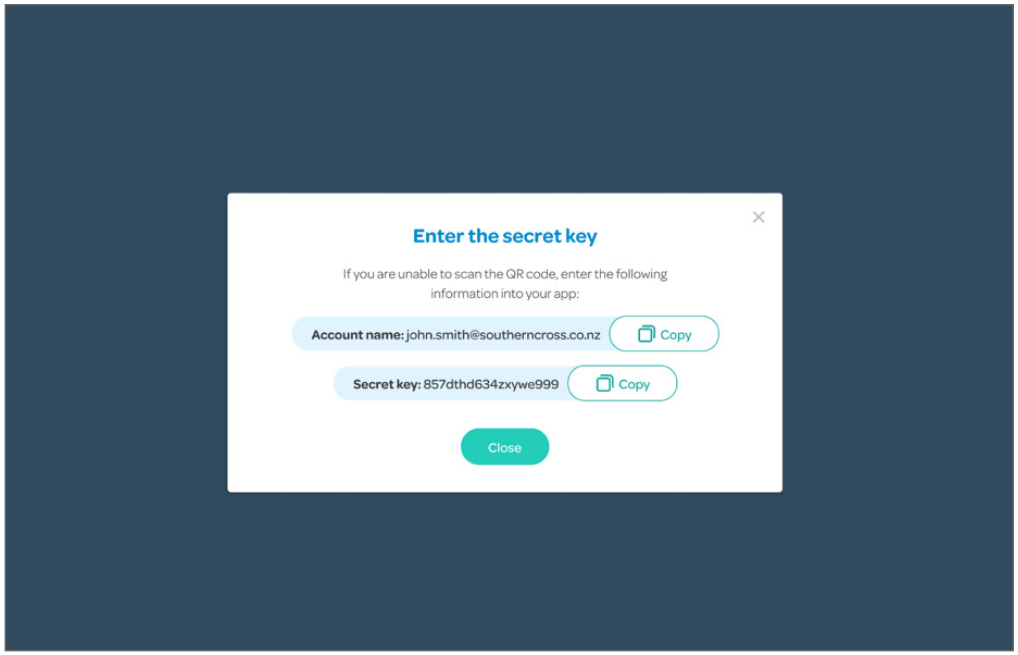


Authenticator app flow

If you enter the incorrect code, you will receive the below error.

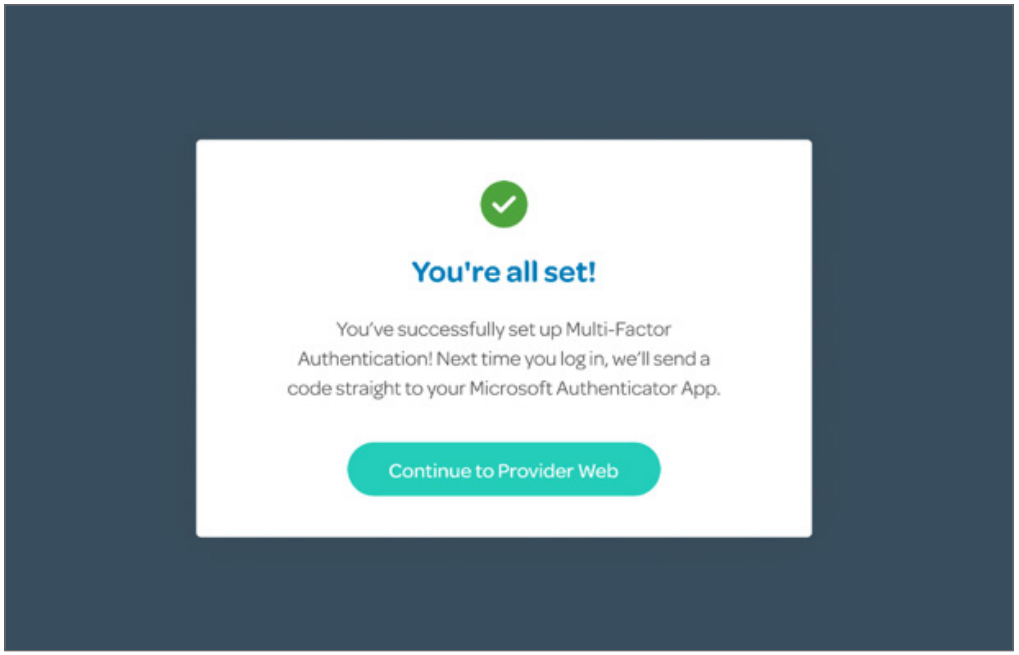


If you have issues with scanning the QR code, you will see the below message.



Authenticator app flow

Once you're set up, you'll receive this message.

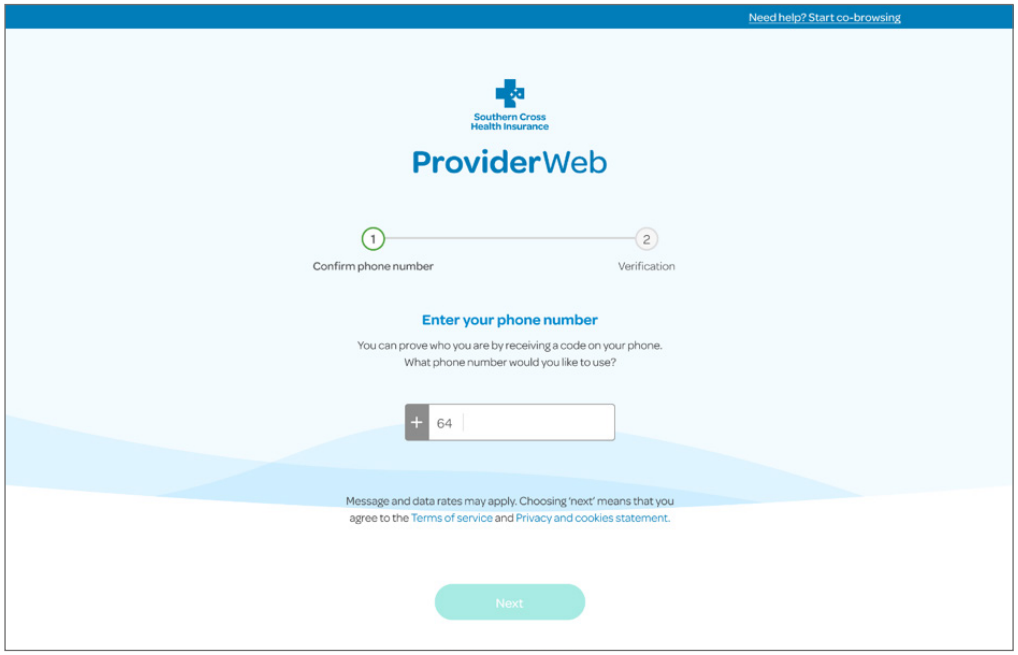


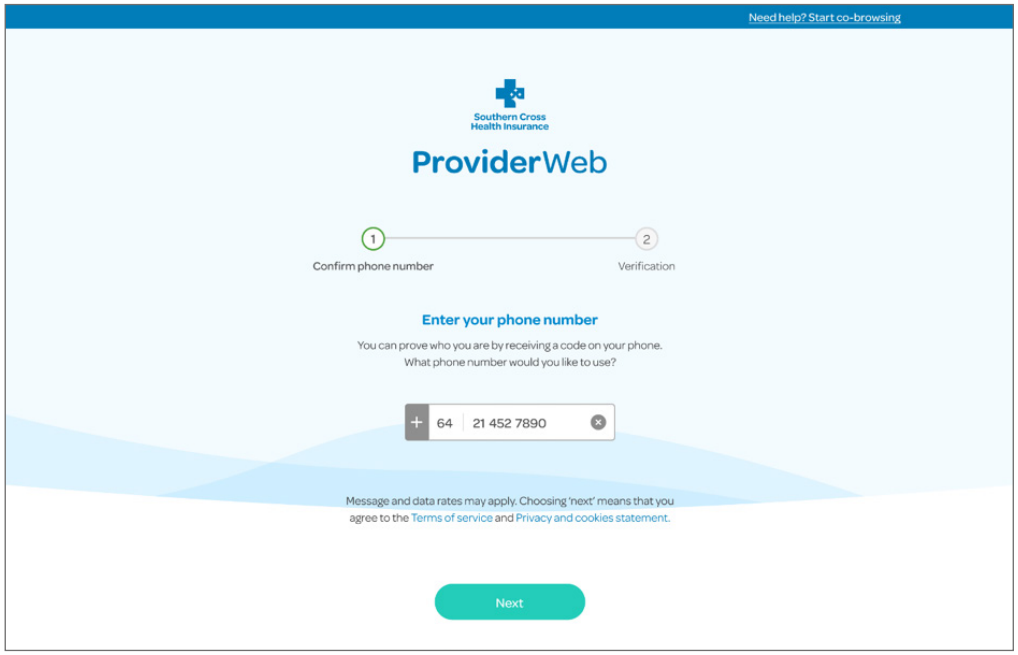
SMS (text) flow

Below is the flow you will follow if you choose SMS as your preferred MFA option.

Enter the phone number you will be using.

The **'next'** option will become clickable once you enter the correct phone number.

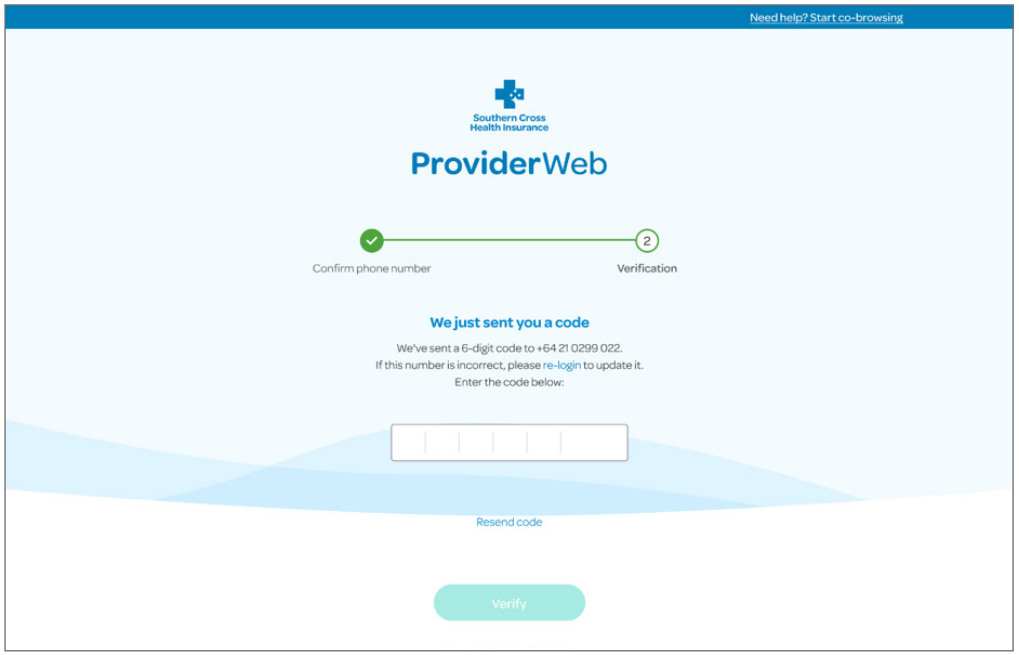


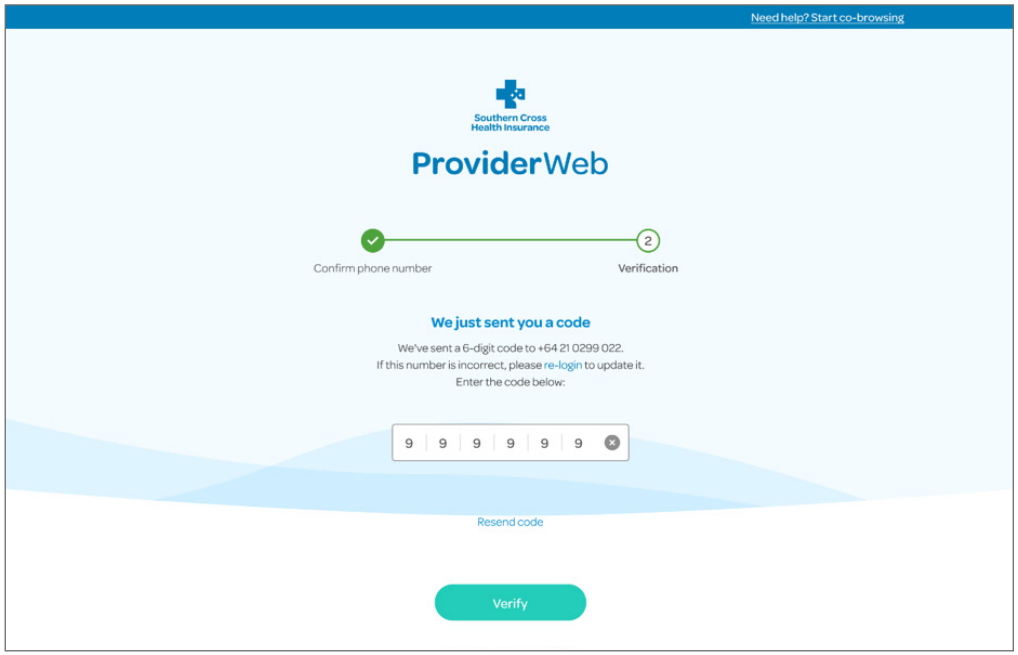


SMS (text) flow

Enter the verification code that you receive via text.

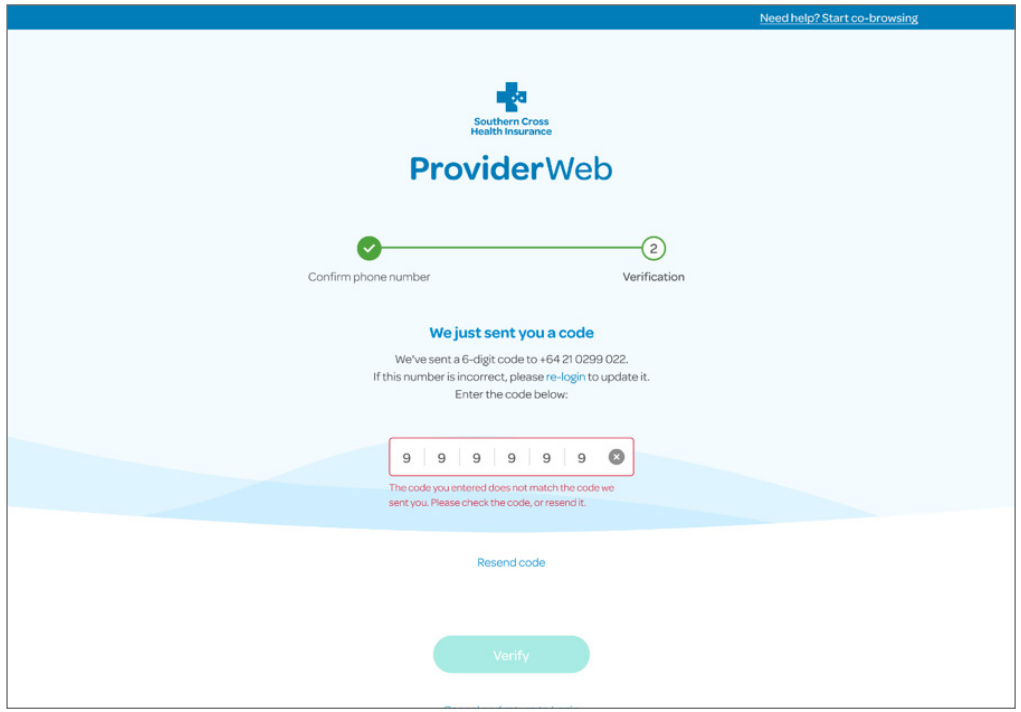
The **'verify'** button will become clickable once you enter the correct code.



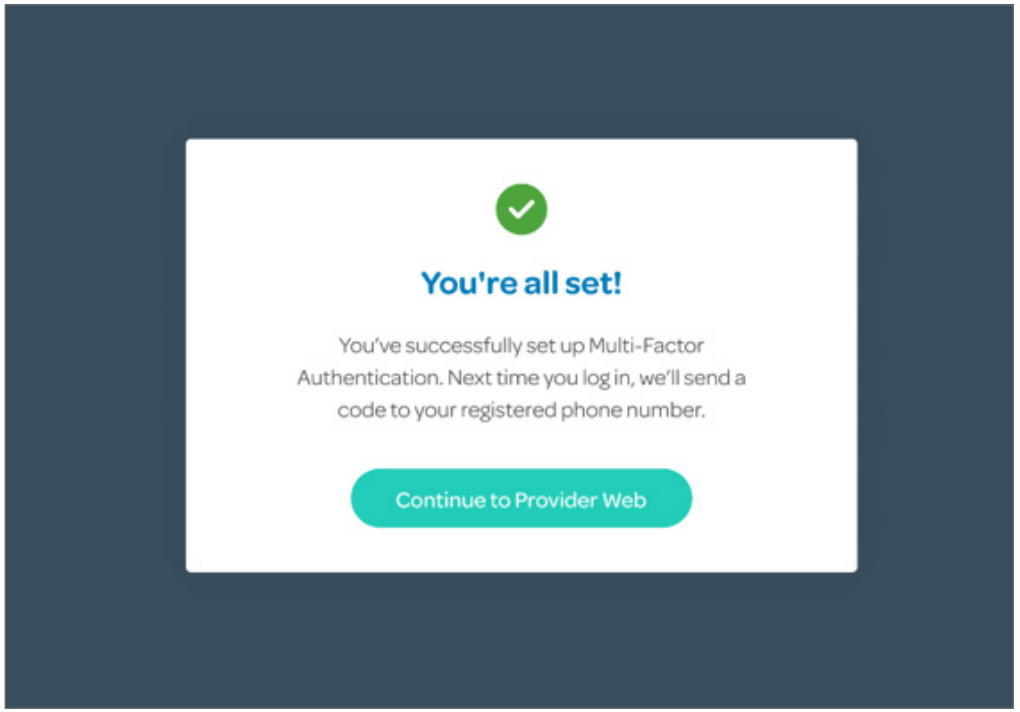


SMS (text) flow

You will receive this error if you enter in the wrong code.

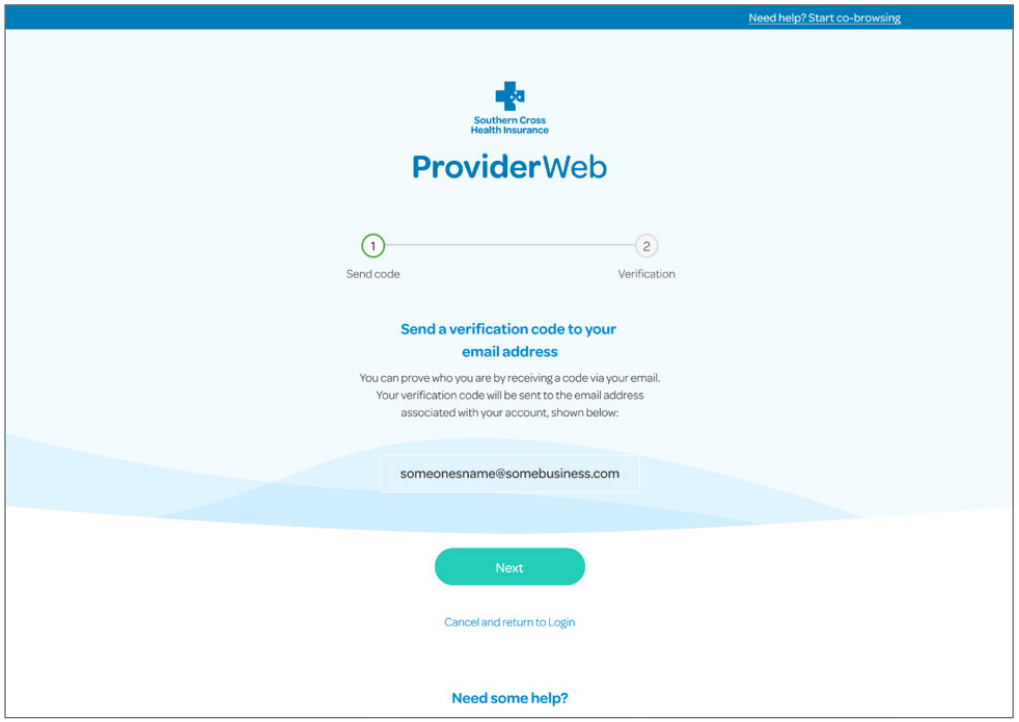


You will receive this success message once you're set up.

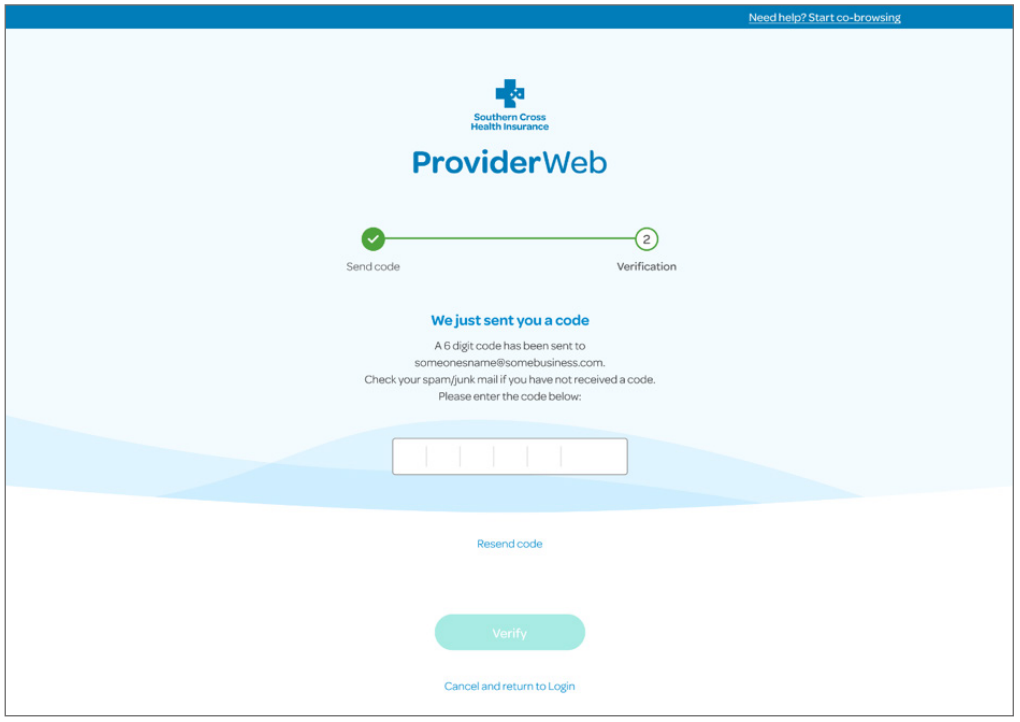


Email flow

Below is the flow you will follow if you select email as your preferred MFA option.

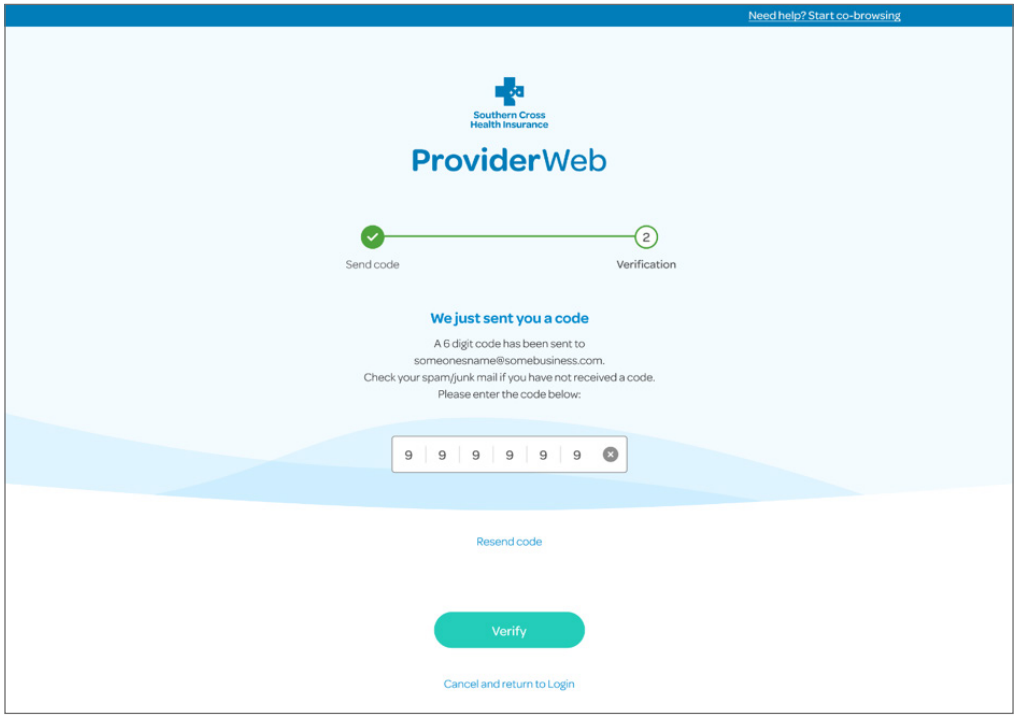


Enter the 6-digit verification code that has been sent to your email address.

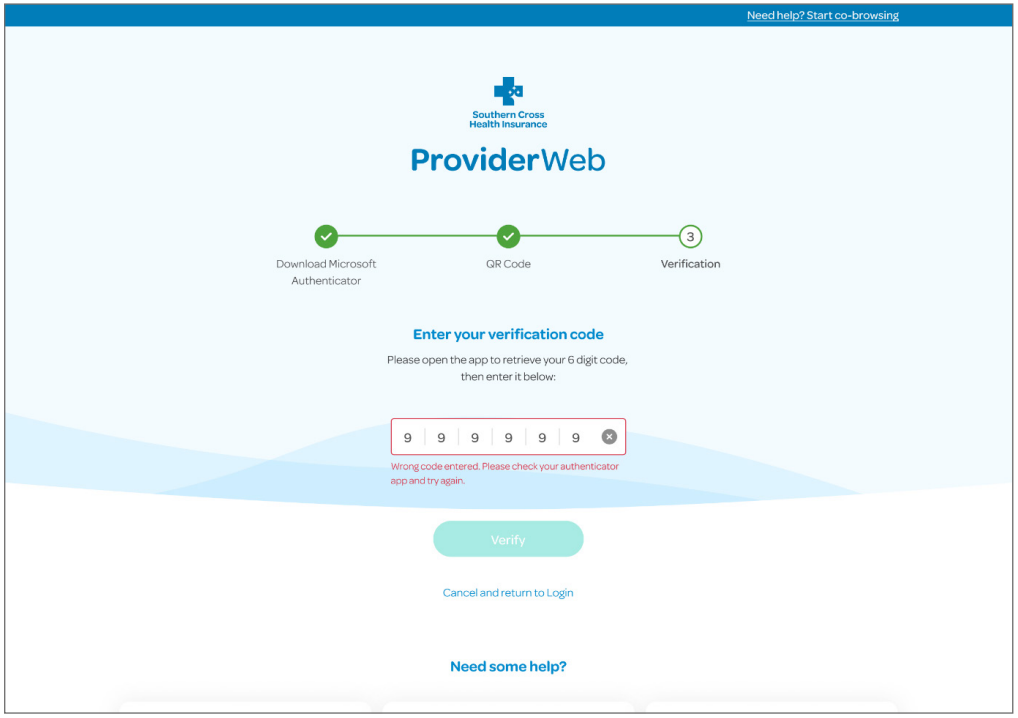


Email flow

Once the correct code is entered, the **'verify'** button will become clickable. Click **'verify'** to continue forward.



Email flow



Important information about shared email boxes - impact on verifying your identity

If you choose to verify your identity via email, your experience will be optimal if you have one login email address. If you share logins or email addresses the experience is not ideal – this may cause delays in your login journey.

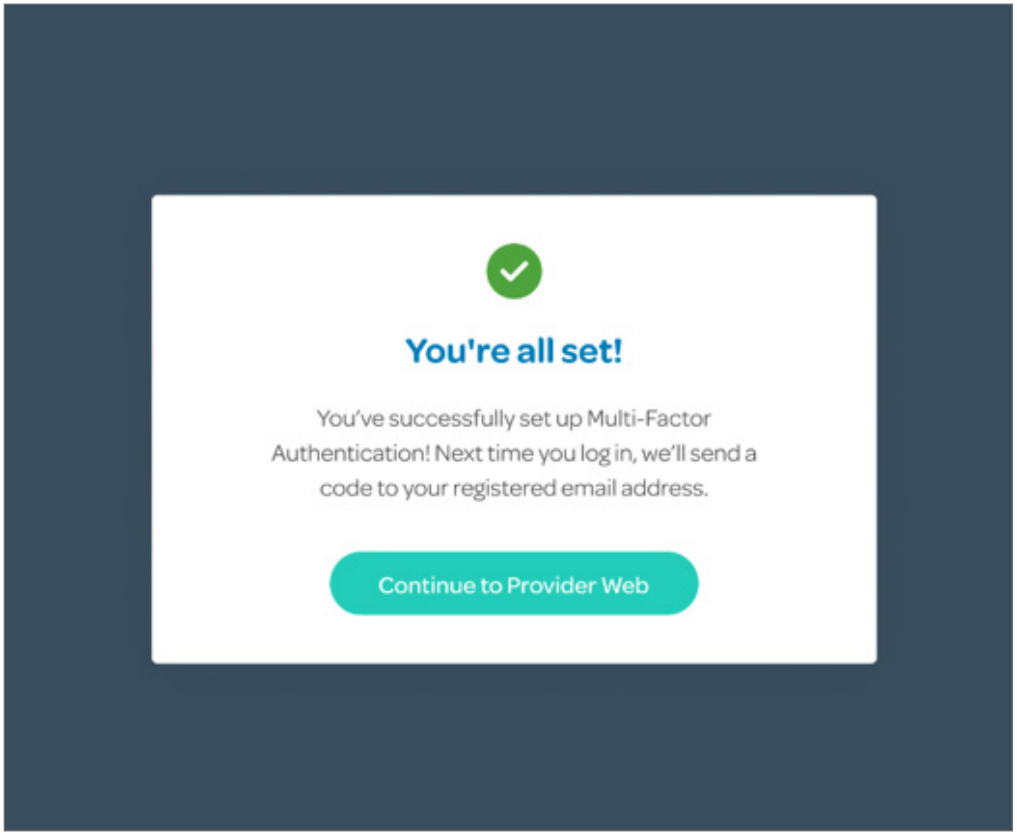
- The most recent code generated is the valid code and invalidates any generated before. For example, if Susan and Emily are authenticating at the same time and Emily generates a code after Susan then Susan's code is no longer valid – the code that will work is Emily's. Susan will need to generate a code after Emily has validated and logged in.
- A code can only be used once and one at a time.
- This means you will need to coordinate logins for those who have shared email addresses.

This is the error you will receive if you enter the wrong code. If there are issues with your code click 'resend code'.

Email flow

Once you correctly verified your email address, you'll be set up.

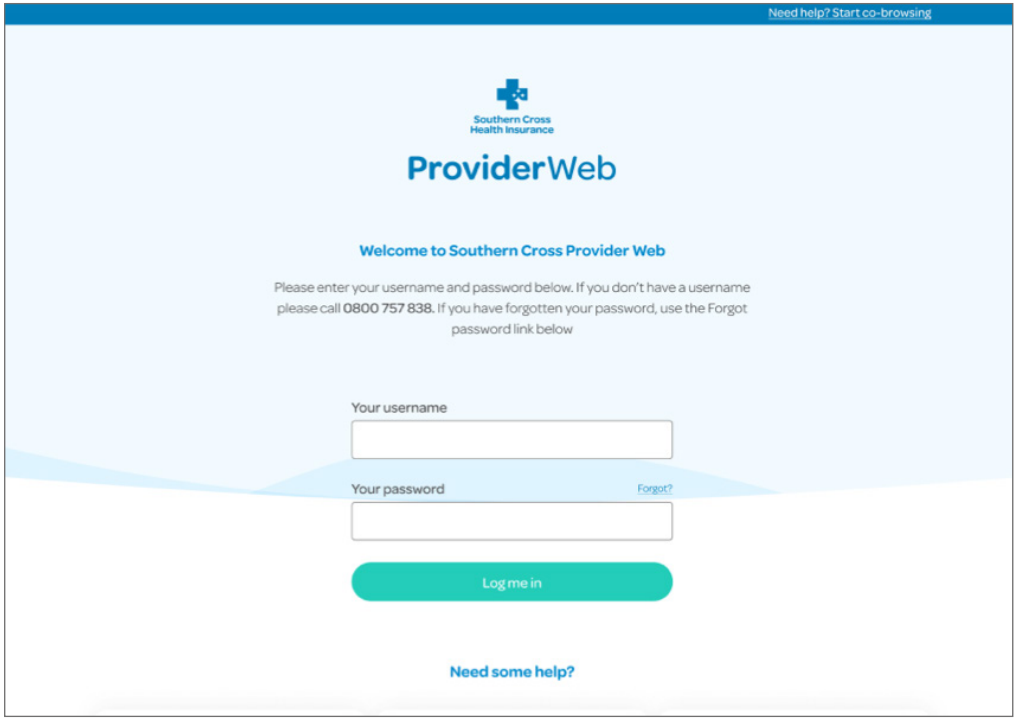
Click **'Continue to Provider Web'** to log in.



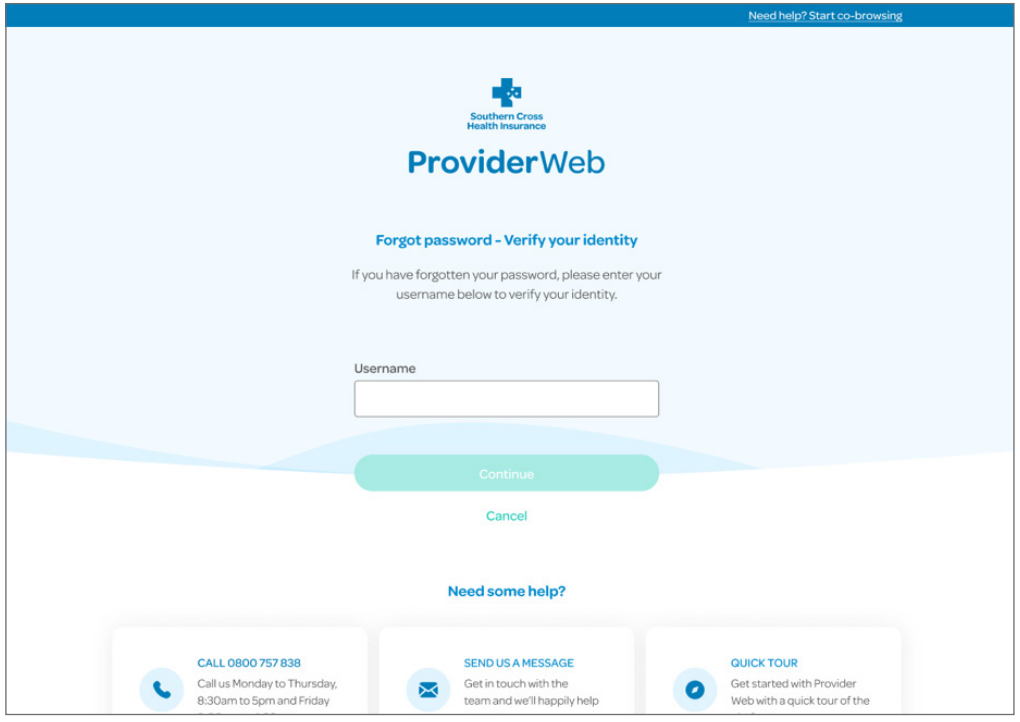
Setting up MFA when you don't know your password

Below is the flow for when you are trying to set up your MFA but do not remember your current password.

Select **'Forgot'** on the login page.

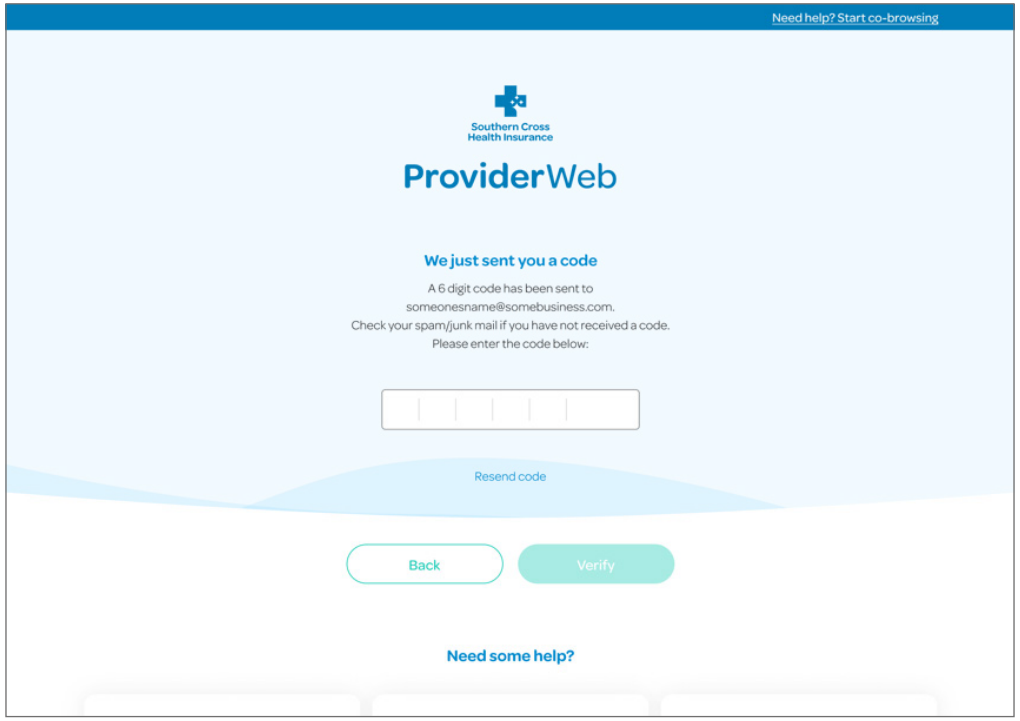


Enter your username and click **'Continue'**.



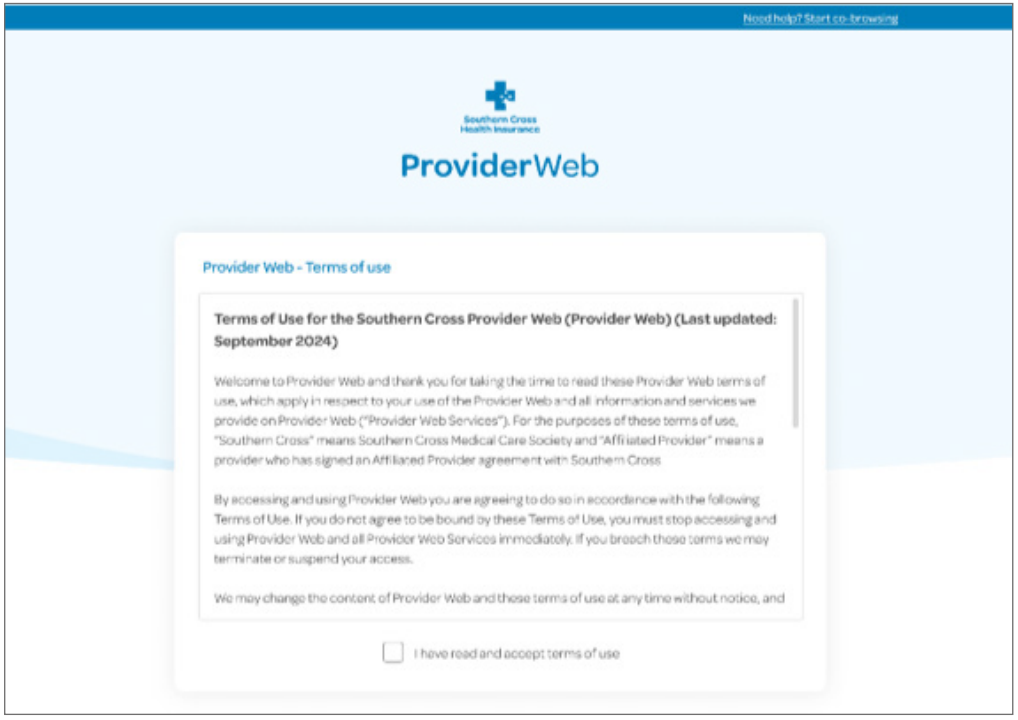
Setting up MFA when you don't know your password

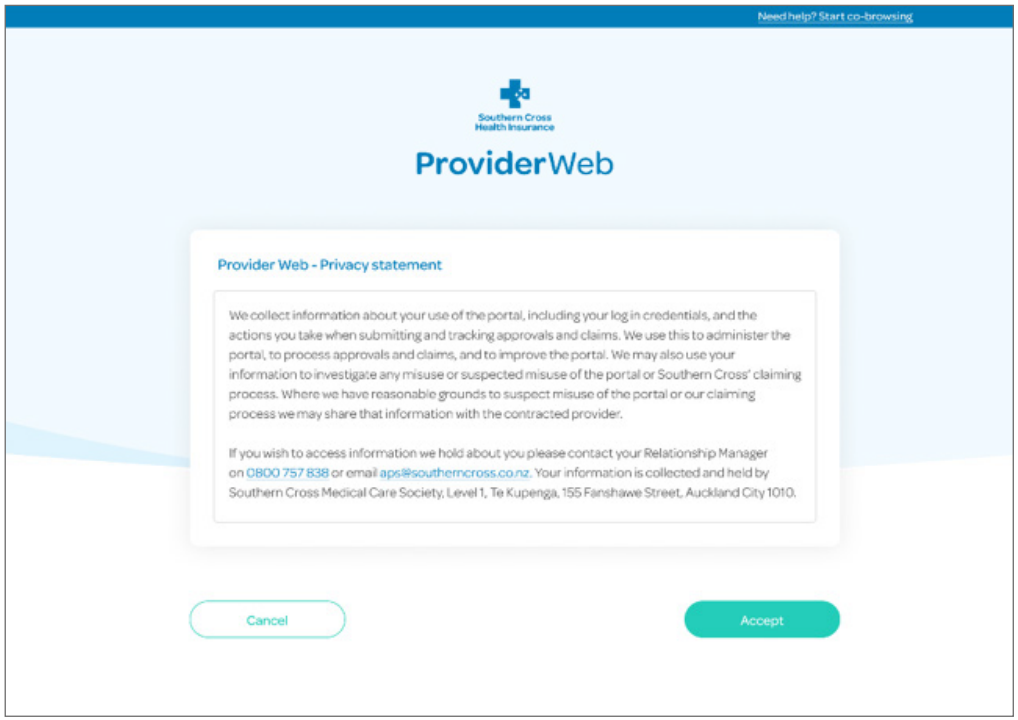
Enter the 6-digit verification code that has been sent to your email address.
Once the correct code is entered, the '**verify**' button will become clickable.
Click '**verify**' to continue forward.



Setting up MFA when you don't know your password

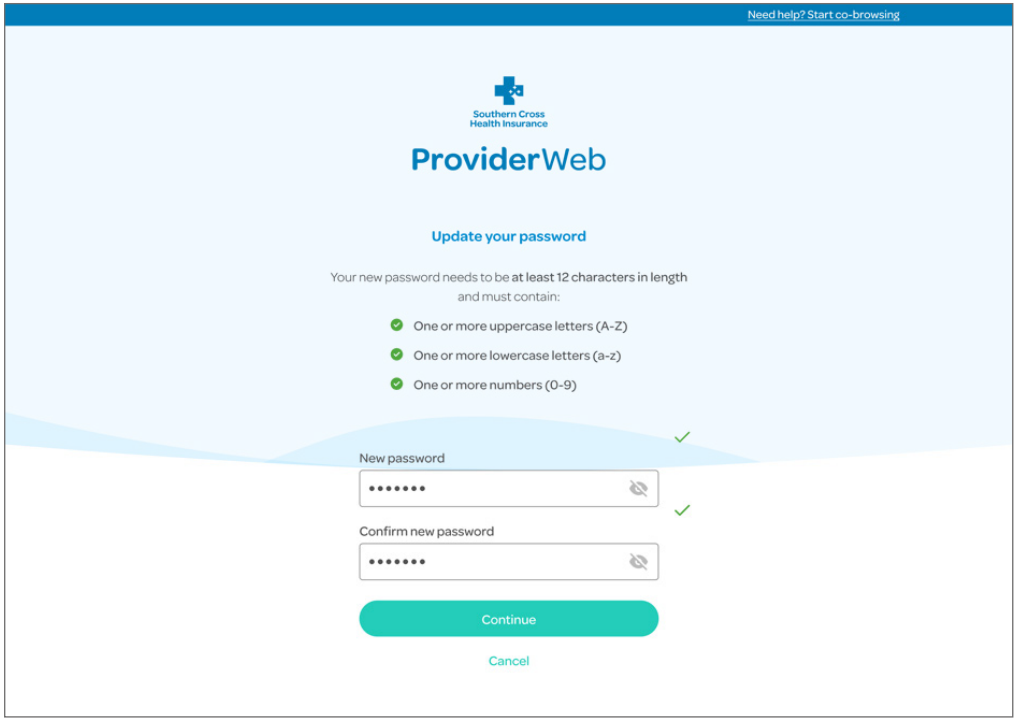
Please read and accept the terms of use and the privacy statement.



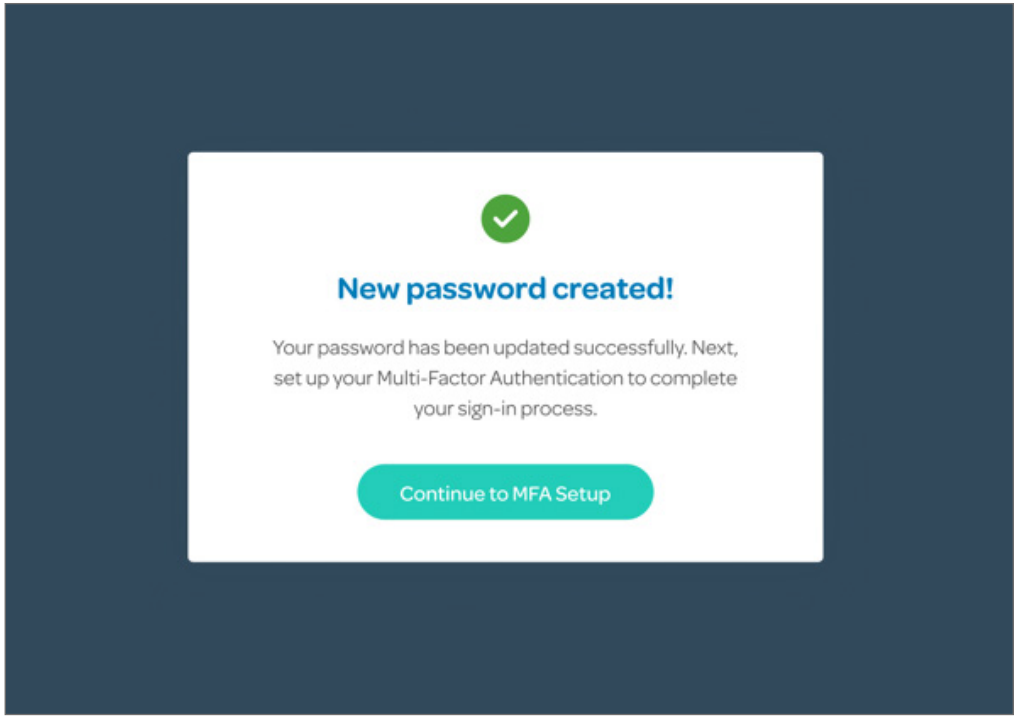


Setting up MFA when you don't know your password

Enter your new password twice. If it meets the requirements then you will see two green ticks.



Once you have set a new password you will be able to continue and set up your MFA.



FAQs

What is MFA?	Multi-factor authentication (MFA) is a method of authentication that uses two or more factors of identity to confirm that a person is who they say they are.
Why do we need MFA?	MFA is now required for Provider Web as it has sensitive member information and medical procedures applied for each member. • Passwords requirements don't meet current best practice to keep them safe. • Danger of ex-employee accessing offsite for years after they leave a provider. Currently these are never disabled and automatically renew.
When signing in, what methods are available to get my pass code?	To receive a one-time pass code all Provider Web users will have a choice between: • Email • SMS • Microsoft Authenticator App
Timeframes	
How long before I have to do this?	MFA will be made mandatory as of May 2025.
What will happen if someone doesn't set up MFA?	If you do not set up MFA, you won't be able to access Provider Web.
How long before my login expires?	After 60 minutes it will automatically end your session after a period of inactivity to protect against unauthorised access.
How many login attempts do I have?	You will be allowed 10 attempts before it starts timing you out. The timeout is 60 seconds. After the 11th attempt it will keep increasing every try up to a maximum of five hours.

FAQs

How often do I need to authenticate?	Every seven days you will need to reauthenticate your login.
Will people who don't log in very often get a notification?	Not in the short term. Notifications will begin later.
Who to contact	
Who do I contact if I don't understand how to set up and use my MFA?	Please review this MFA user guide or if you still need assistance contact your Affiliated Provider relationship manager at: • Phone: 0800 757 838 • Email: aps@southerncross.co.nz • Post: Southern Cross Health Society, Private Bag 99934, Newmarket, Auckland 1149
Other	
Can we use shared emails, usernames, passwords?	• You must have individual usernames and passwords. • You can share emails, but you must use unique usernames for those sharing the same email address. • If using SMS to authenticate you will need to use unique phone numbers.
I haven't received my code – what's happening?	Please wait for the code, it could take a few minutes. Also please check your junk/spam folder if using email. If the code has not been received, please click the 'resend code' button to try again.
The code I received didn't work, why?	Please make sure that every space is filled with a number when verifying your code.

FAQs

What happens if I lose access to my authentication device?	Contact your relationship manager to reset your account so you can set up your MFA again.
How can I reset my MFA settings if I change my MFA device (eg phone or laptop)?	Please contact your relationship manager for help.
Can I disable MFA if I find it inconvenient?	No. MFA is a mandatory requirement for those accessing Provider Web.
What if I forget my password and lose my chosen MFA method?	Contact your relationship manager to reset your MFA and then use the 'Forgot' password link on the login page.
What should I do if I receive an MFA request that I didn't initiate?	Please contact your relationship manager.
Can I choose another MFA option if my chosen method fails?	If it fails and you need to change your MFA method, please contact your relationship manager. They will help you reset your MFA.
Is MFA required for all Provider Web users at my organisation?	Yes, this is required.
Can I change my password once I am logged into Provider Web	To change your password, you will need to logout of Provider Web and click the 'Forgot' password link on the login page.

We're here to help

Contact information

If you need help, please give us a call on:
0800 757 838 or email us at aps@southerncross.co.nz