



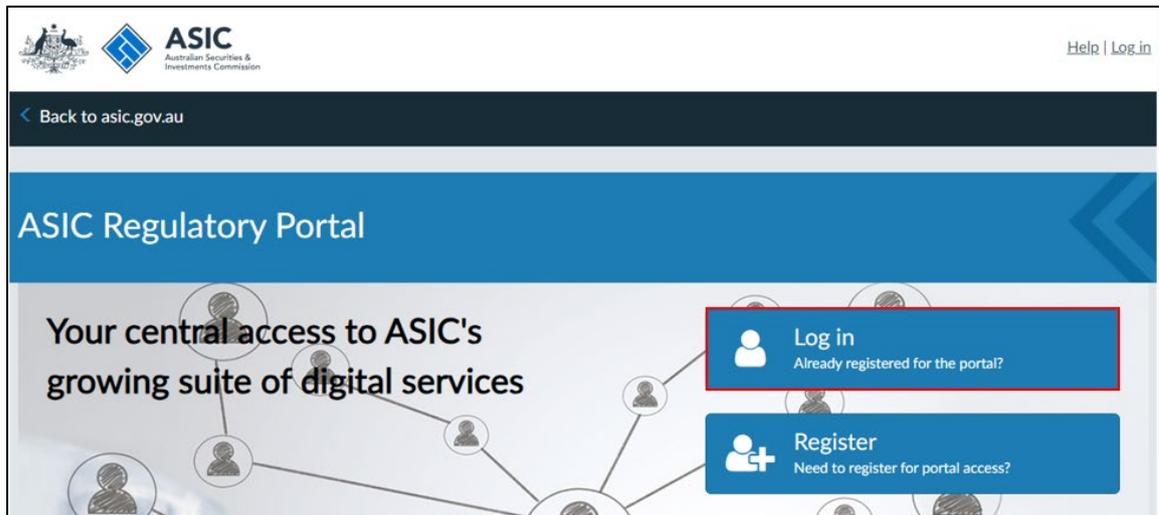
How to add an authentication app

ASIC Regulatory Portal user guide | Version 1.0, May 2025

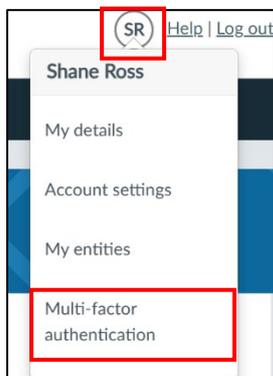


While it is not mandatory, users can log in using an authentication app for added security. Alternatively, they may continue to log in using email authentication.

1. Log in to the [ASIC Regulatory Portal](#).



2. Once you have logged in, click on **your initials in the top right of the banner**. This will reveal a drop-down menu. Click **Multi-factor authentication**.



- This will direct you to the **multi-factor authentication settings**.

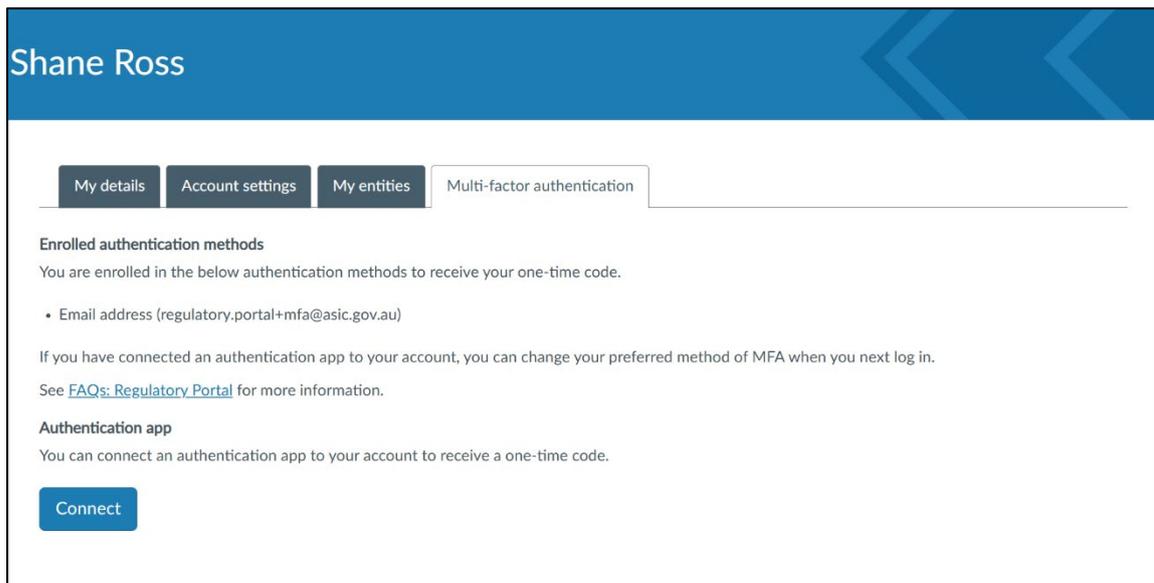


Table 1 shows the differences between the two multi-factor authentication methods.

Table 1: Further information about multi-factor authentication methods

Available authentication methods	Information on authentication methods
Email authentication (default method)	A one-time authentication code is sent to the email address used as your ASIC Regulatory Portal username. This is the default multi-factor authentication method, and it cannot be removed.
Authentication app (optional)	An authentication app is an application installed on a computer or a mobile device, such as a phone or tablet. The app generates a one-time code for authentication. The code can be generated by the app without access to the internet. This method of authentication is only available if you have set it up in your portal account.

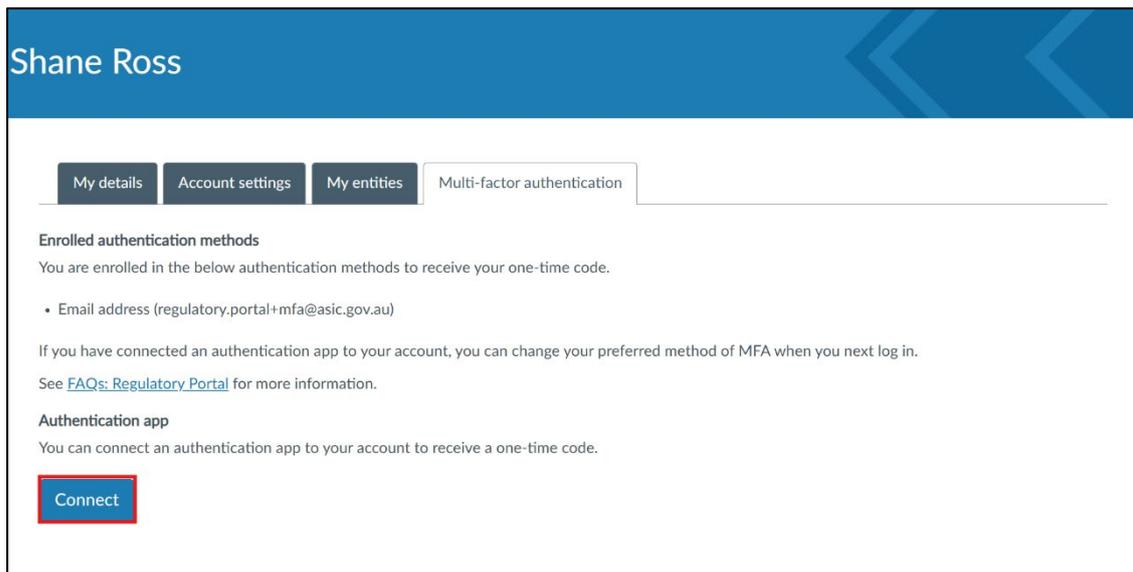


What authentication apps can I use?

You can use any third-party authentication app of your choice. However, we recommend that you use a reputable app such as Microsoft Authenticator or Google Authenticator.

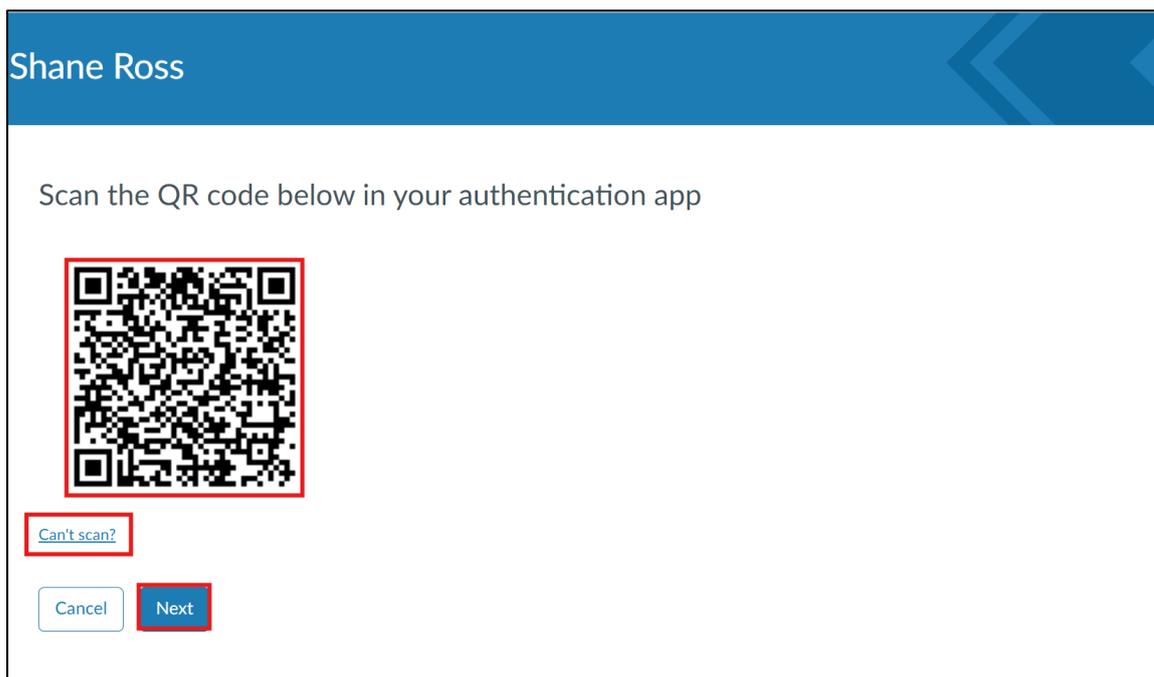
You will need to have already downloaded your preferred authentication app to your mobile device before moving on to the next steps.

4. On the **multi-factor authentication** tab, click the **Connect** button. This will reveal a QR code.

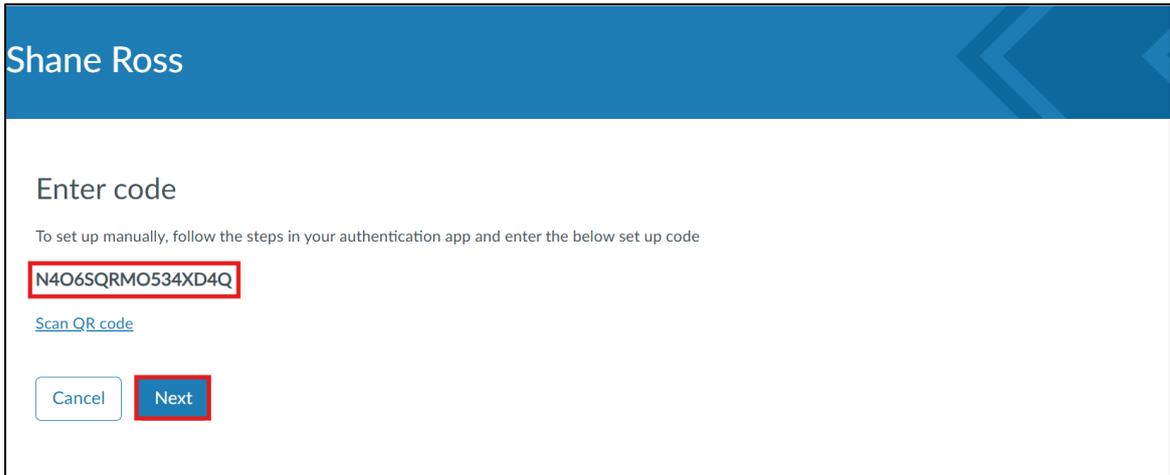


5. **Scan the QR code** using the authentication app. Follow the steps on your app to generate a one-time code. Move to Step 7.

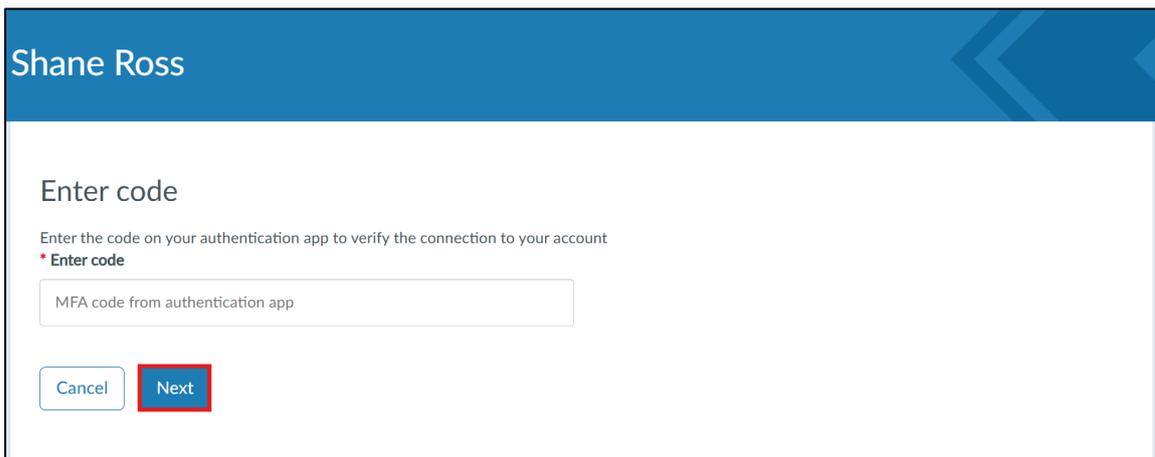
If you cannot scan, click **Can't scan?** and move to Step 6.



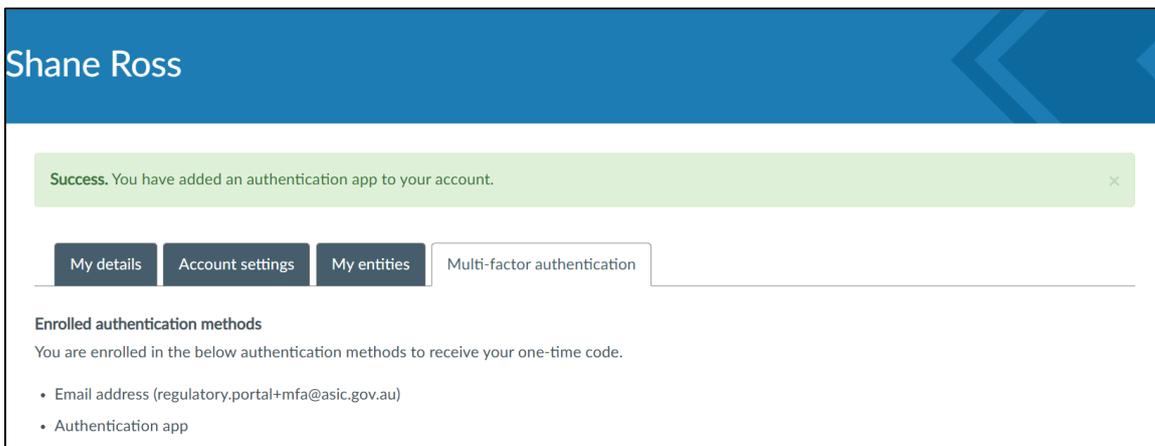
6. Enter the **set up code from the portal** in your authentication app when prompted by your app. Follow the steps on your app to generate a one-time code.



7. Click **Next**.
8. Enter the **one-time code shown on your authentication app** in the text box and click **Next**.



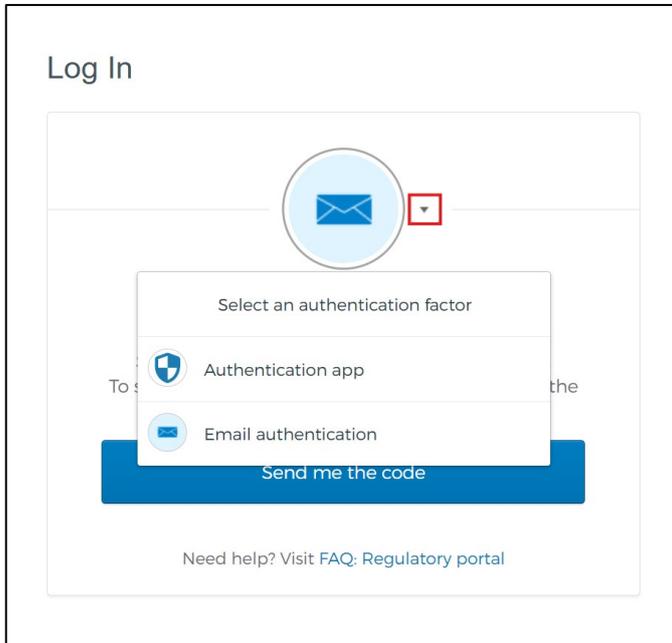
9. A **success message** will display, confirming your account has connected to an authentication app.



10. An **email will be sent to the user** confirming that the authentication app has been added.



When you attempt to log in after adding the authentication app, click on the **toggle arrow next to the icon** on the authentication page, and then click **Authentication app** or **Email authentication** if you would like to update your preferred method of authentication.



What if there is an issue with the authentication app?

If there is an issue with the authentication app, either contact the publisher of the app for support or switch to email authentication to log in.