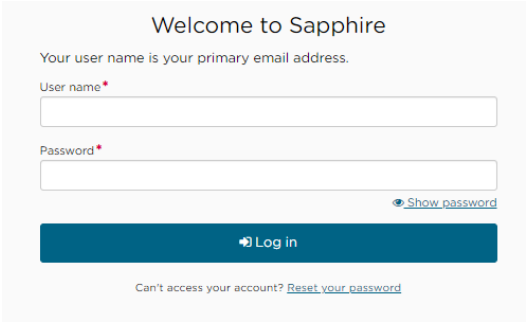
How to Setup Multi-Factor Authentication (MFA) in Sapphire

Australian Government
National Health and Medical Research Council

Note: You will need to download the 'Google Authenticator' or 'Microsoft Authentication' app onto your smartphone through the Android Play or Apple App store.

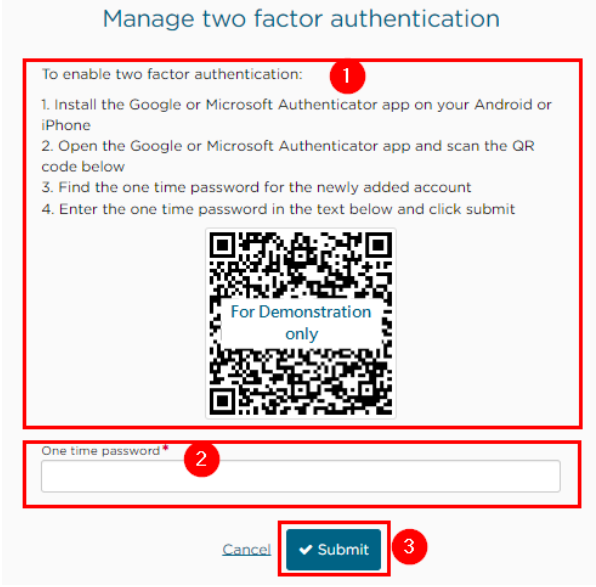
Step 1

From a desktop computer or laptop web browser visit the Sapphire login page and enter your username and password in the fields provided and click "**Log in**".



Step 2

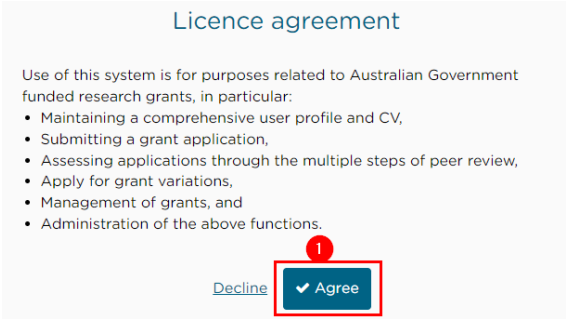
1. Follow the instructions provided on the screen and scan the QR code through your Authenticator app. For information on installing an Authenticator app see section "*Installing and using an Authenticator app*".
2. Find the one-time password for your account and enter in the text field below.
3. Once you have entered your code, click **Submit**.



Step 3

A "Licence agreement" notice will appear on your screen.

1. Click **Agree.** This will log you into your account.



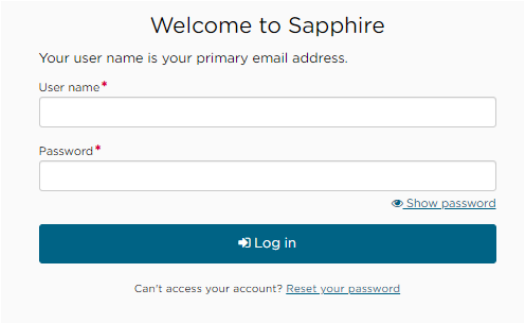
BUILDING
A HEALTHY
AUSTRALIA

How to login to Sapphire with MFA

Note: You will need to download the 'Google Authenticator' or 'Microsoft Authentication' app onto your smartphone through the Android Play or Apple App store.

Step 1

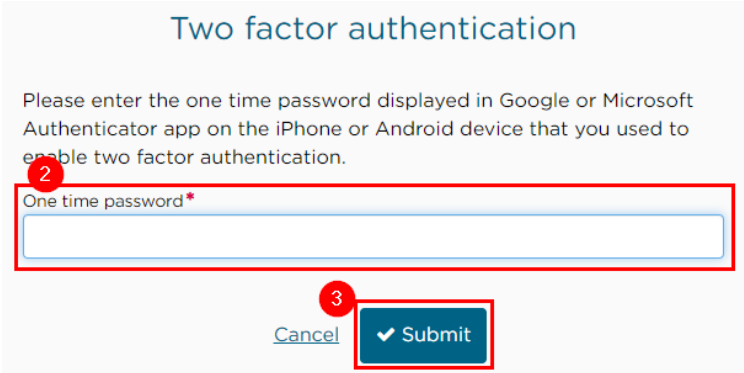
From a desktop computer or laptop web browser visit the Sapphire login page and enter your username and password in the fields provided and click "**Log in**".



Step 2

Provide a one-time password.

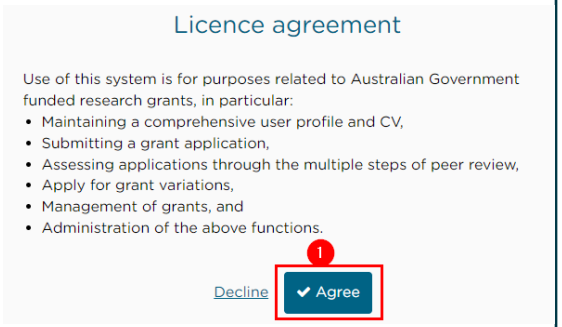
1. Open your Google/Microsoft Authenticator app installed on your device.
2. Find the one-time password for your account and enter in the text field below.
3. Once you have entered your code, click **Submit**.



Step 3

A "Licence agreement" notice will appear on your screen.

1. Click **Agree.** This will log you into your account.

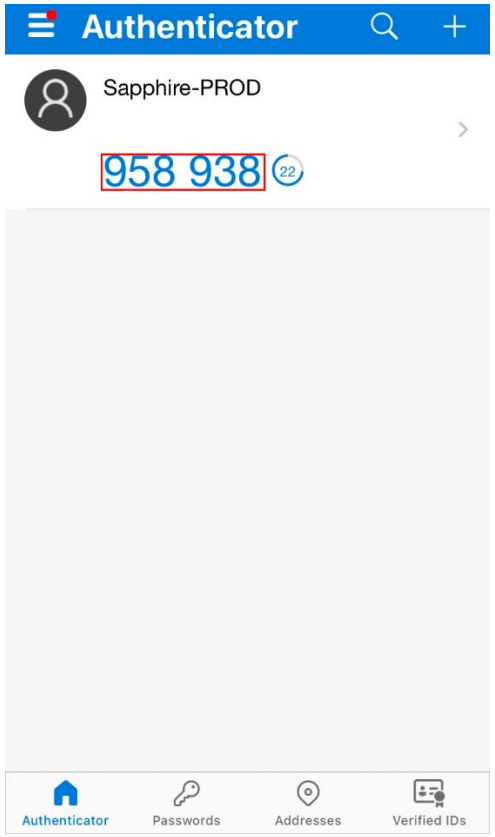


Note: Sapphire MFA is compatible with the **Google Authenticator** or **Microsoft Authenticator** apps. Please, note that it is not compatible with the Chrome web browser extension Authenticator.

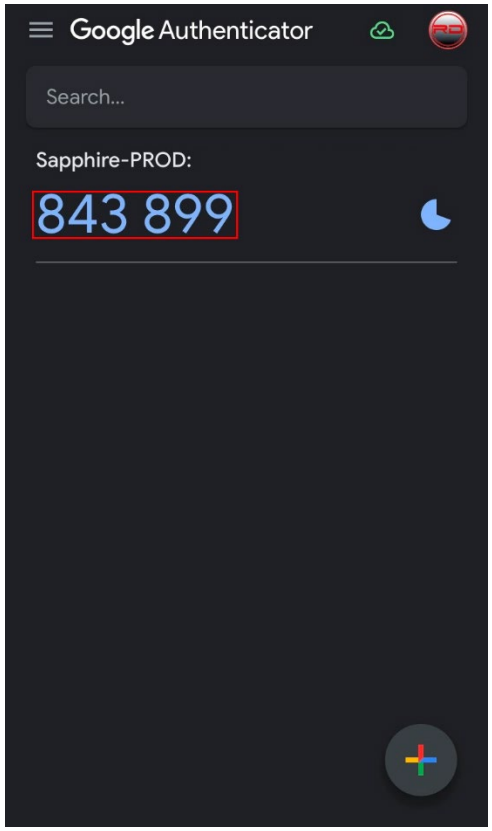
	Google Authenticator	1. Download and install the Google Authenticator app onto your smartphone/tablet through the Android Play store or Apple app store. 2. Open Google Authenticator and click on the + sign on the bottom right of the app screen to add a new account. 3. Select the option to '*Scan a QR code'*. 4. Scan the Sapphire QR code (see the section '*How to setup MFA in Sapphire',* step 2) to add Sapphire+Prod to Google Authenticator.
	Microsoft Authenticator	1. Download and install the app onto your smartphone/tablet through the Android Play store or Apple app store. 2. Open Microsoft Authenticator and click on the + sign on the top right of the app screen and select a type of account (i.e. personal, work, other). 3. Select the option to '*Scan a QR code'.* 4. Scan the Sapphire QR code (see the section '*How to setup MFA in Sapphire',* step 2) to add Sapphire+Prod to Microsoft Authenticator.
Authenticator for Google Authenticator	Chrome web browser extension Authenticator	Not compatible with Sapphire MFA.

Below is an example of a one-time password for the Microsoft Authenticator and Google Authenticator apps.

MS Authenticator



Google Authenticator



Why is MFA mandatory?

MFA meets Australian government security requirements by providing an extra layer of security. Otherwise known as two-step verification, MFA uses a second step like a one-time password on your phone to make it harder for others to break into your account. MFA is a mandatory requirement for all Sapphire accounts.

What if I accidentally uninstall my Authenticator app or delete my Sapphire MFA instance from the app?

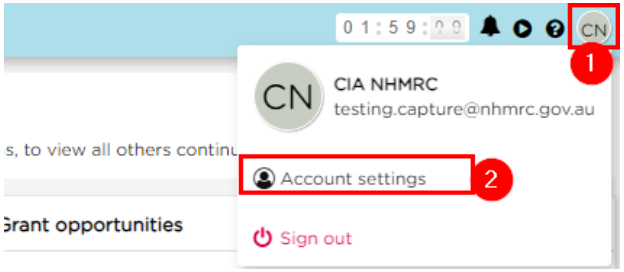
Contact the Research Help Centre (RHC) on help@nhmrc.gov.au who will be able to reset MFA for your account. Once your account's MFA has been reset, you will need to set up MFA again by scanning the QR code on the login page through an Authenticator app on your phone/tablet.

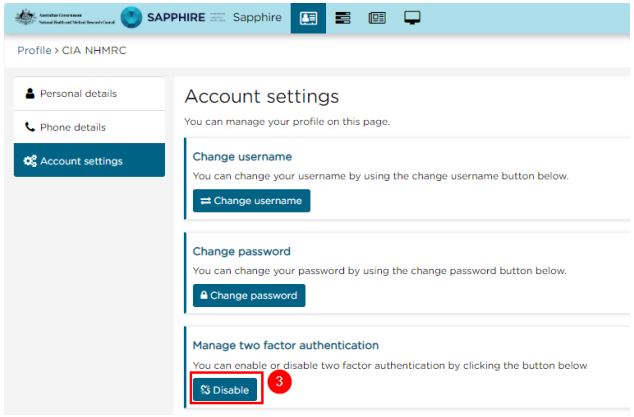
Alternatively, if you are still logged into Sapphire you can disable/enable this yourself through your 'Account settings'. See '*How do I re-register for MFA*' section below.

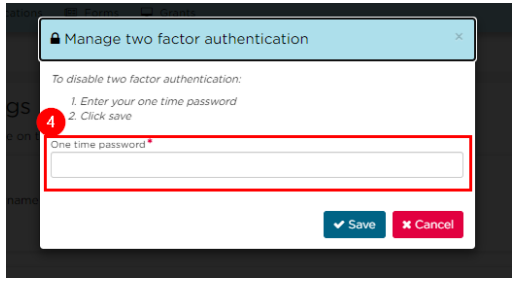
How do I re-register for MFA (i.e. on a new device?)

If you want to un-register MFA from your old device and re-register it on a new one you can do one of the following:

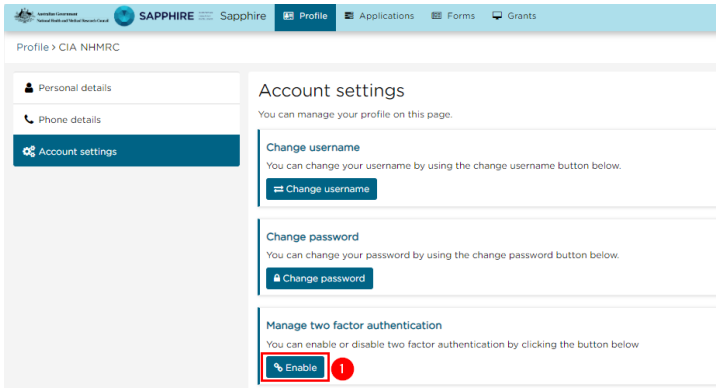
1. While logged into Sapphire, click on your avatar icon on the top-right corner and select '*Account settings*'. From there you will be able to '*Disable*' MFA in the '*Manage two factor authentication*' section. Sapphire will prompt you for a one-time password before disabling MFA for your account.

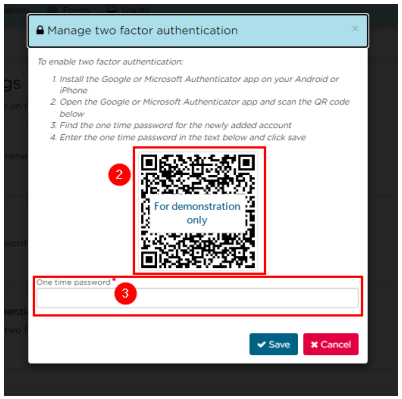






Once MFA is disabled you can Click on '*Enable*' in the Account settings '*Manage two factor authentication*' section and scan the new QR code on your new device, or alternatively a new QR code will pop-up upon your next log-in and prompt you to re-register.





2. Alternatively, you may contact the Research Help Centre (RHC) on help@nhmrc.gov.au who will be able to reset MFA for your account. Once reset, the next time you log into your Sapphire account it will prompt you with a new QR code to scan through an Authenticator app on your phone/tablet.

Can I setup MFA for Sapphire on more than one device?

You can only scan the QR code once to setup Sapphire MFA and therefore it will be installed on the device you scan the QR code on. Whether you can use the same instance of 'Sapphire+Prod' MFA on another device will depend on your phone/tablet. For instance, Google Authenticator may let you import your already existing MFA instances from one device to another within your Google account. The best way to use Sapphire MFA is to have it installed on your phone which you are more likely to always carry on you.

Are there other ways to authenticate my Sapphire account?

The only way to obtain a one-time-password for your Sapphire account is through the Microsoft Authenticator or Google Authenticator app. Sapphire will not work with the Chrome web browser extension Authenticator app.

Where is my one-time password?

If this is the first time you are setting up MFA for your Sapphire account then you will need to download and install an Authenticator app (Microsoft Authenticator or Google Authenticator) on your phone/tablet through the Android Play or Apple app store.

Open the Authenticator app on your device and add a new account by scanning the QR code provided on the Sapphire login page (see section '*How to setup MFA in Sapphire'*). This will add the account: Sapphire+Prod to your Authenticator app.

Once you have added 'Sapphire+Prod' to your Authenticator app your one-time password will appear there (see section '*Example of Authenticator app screens*' for an example of what a one-time password looks like).

For security reasons the one-time password has a time limit before it expires and another code is immediately generated. You will need to submit your one-time password in the Sapphire login page before it expires in the app.

Why is my one-time password not working?

The most common reasons why a one-time password may not work are:

- The one-time password has timed out. Make sure that you are entering and submitting the one-time password in Sapphire before it times out (approximately 30 seconds) or you will need to enter the new one that the Authenticator app generates.
- Sapphire login session in the web browser is timing out.
    - The Sapphire login page has about a 20-minute time-out session from when the username and password has been entered before it times-out and the password/username needs to be re-entered.
    - If you are attempting to setup MFA for the first time in Sapphire and the Sapphire login session in your web browser has timed-out before you submitted the one-time password you will need to remove the Sapphire+Prod account from your Authenticator app and re-scan the QR code to re-add it.
- The time may not be correctly synched to your Authentication app.
    - For Android devices using Google Authenticator: To set the correct time:
        - On your Android device, open the Google Authentication app.
        - Select the menu icon (three dots) then Settings> Time correction for codes >Synch now.
        - The app will confirm the time has been synched. This will only affect the internal time of your Google Authenticator app and will not change your device's Date and Time settings.

- For Android devices using Microsoft Authenticator:
  - Make sure the date and time on your device are correct and are being automatically synced. If the date and time is wrong, or out of sync, the code won't work. You can set your device to automatically sync the date and time through your device's settings.

- Make sure that your device supports the Microsoft and Google Authenticator apps (Android 8.0+ and IOS 15+). For the best MFA experience it is recommended that users have the most updated Android/IOS version installed on their devices and that the device has enough memory space available to run the MFA Authenticator app.