Australian Government
Australian Research Council

RGS

Multi-factor Authentication (MFA) Functionality

Introduction

The ARC has endorsed Multi-factor Authentication (MFA) functionality when accessing ARC Systems including RMS and SEER. MFA will also apply to other entities instances of RMS, including DESE, Defence and ONI. MFA adds another layer of protection to the RMS and SEER sign-in process. Users will be asked to provide additional verification by receiving a code via an Authenticator App, such as on a phone or other device, and entering that code into RMS or SEER as a second tier of identification.

As part of the ARC's compliance with the Information Security Manual (ISM) and Essential 8, MFA will become mandatory for users with privileged access from 30 June 2022 and optional for other users. Users with privileged access include Users with a staff role that entitles users to additional system access, for example staff of Government entities (ARC, DESE, ONI and Defence) and Research Office/Lead Agency staff involved in grants administration.

Passwords will remain a minimum of 14 characters, but the length of time between the mandatory password reset will be 12 months.

MFA will be rolled out to other users in the future, however there is the option for all users to opt into this functionality from 30 June 2022.

Key Points

- RMS and Seer is compatible with the latest versions of Google Chrome and Microsoft Edge. The Australian Research Council (ARC) cannot guarantee compatibility with other browsers or older versions of Google Chrome or Microsoft Edge.
- Your email address that you registered with is used to log in to RMS.
- ARC is utilising Multi-factor Authentication for RMS and SEER systems from 30 June 2022.
- Your password must be a minimum length of 14 characters and **must** contain at least three of the following categories:
  - lowercase alphabetic characters (a-z)
  - uppercase alphabetic characters (A-Z)
  - numeric characters (0-9)
  - special characters (!@#$%&/=?.,:;\-)
- You must change your RMS password every 12 months.
- If you do not use your account within 90 days, RMS will lock your account. Your account can be unlocked by requesting a Password Reset from any RMS Login Page or by contacting RMS Support.
- By requesting an RMS account and through use of the system, you acknowledge that you have read and understood the Privacy Policy for the relevant RMS instance of DESE, Defence, ONI and the ARC.
- By requesting access to the system, and through your use of the system, you acknowledge and understand that the unauthorised disclosure of official information is an offence under the Crimes Act 1914, and that any breach or disclosure will be referred to the Australian Federal Police for prosecution.
- Issues with account creation should be reported to the RMS Support within the ARC.

Set-up Multi-factor Authentication (MFA) functionality:

a) To add MFA to your profile from the Action Centre select Personal details
b) Under your email address select MFA Settings:

Figure 1 MFA Settings button

c) You will be required to download and install a Multi-Factor Authentication app on your mobile device through the Google Play or Apple App Store. Or on you desktop or laptop through a web-based browser for example: [Authenticator - Chrome Web Store (google.com)]

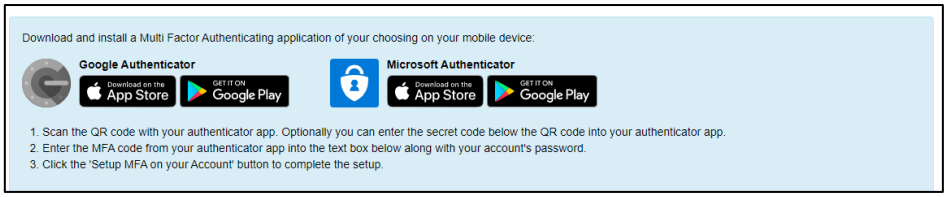

Figure 2 MFA Download app

d) Once you have downloaded the MFA App on your device go back to RMS and select '*Generate New MFA QR Code*'.

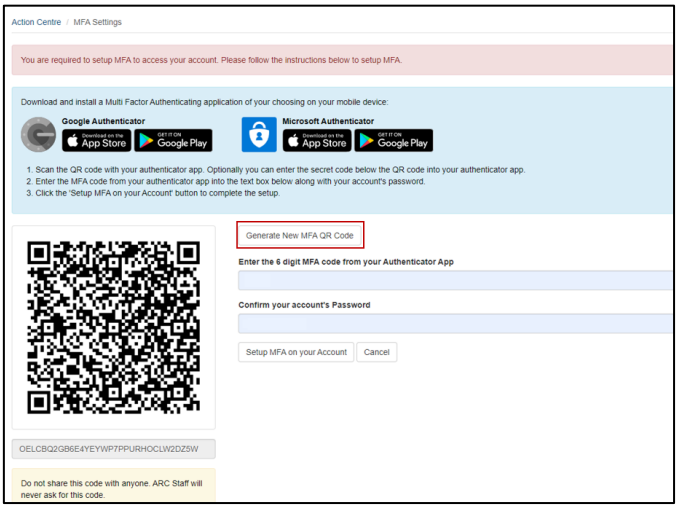

Figure 3 Generate new MFA QR code button

e) Scan the QR code on the screen or enter the code below the QR code. This will send a code to the app on your phone.

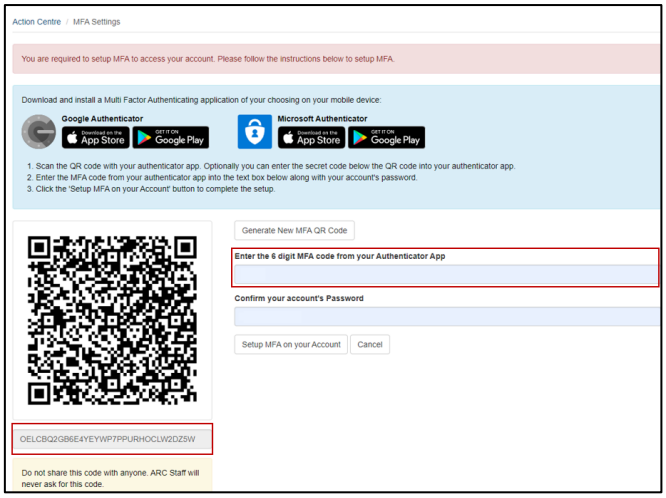

Figure 4 MFA code below the QR code to be entered

f) Enter the MFA six-digit code from the app into the text box and your password.

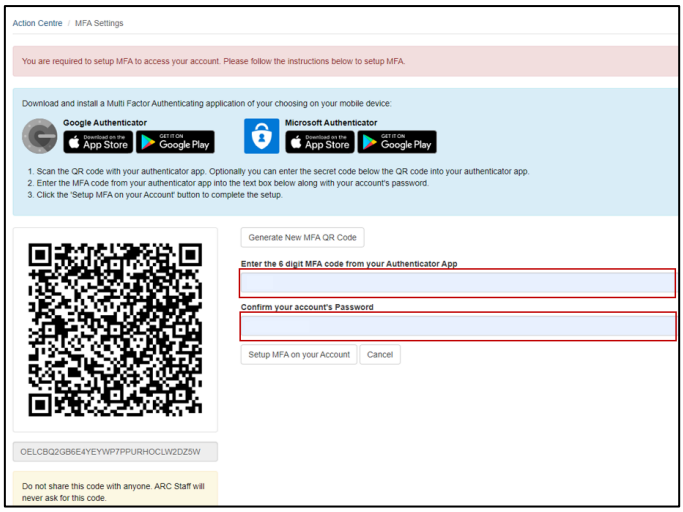

Figure 5 Code and password from the app fields

g) Click the 'Set-up MFA on your account' button.

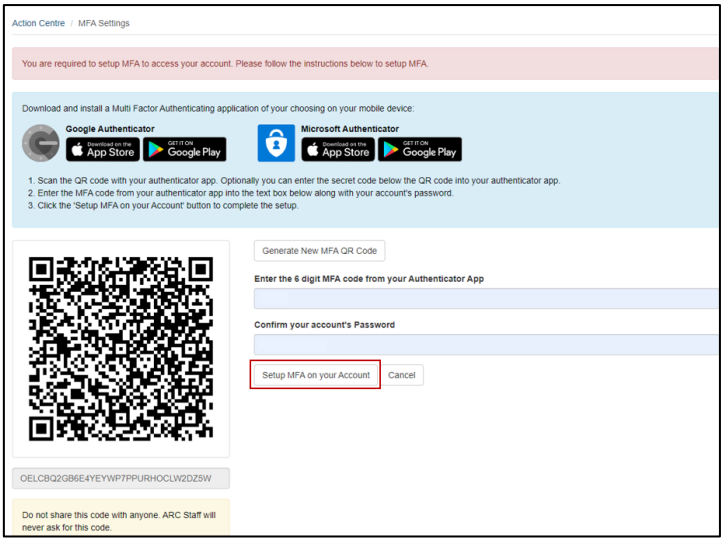

Figure 6 Set up MFA on your account button

h) Once MFA is set-up on your RMS account you will see the following message ‘MFA has successfully been added to this account’.

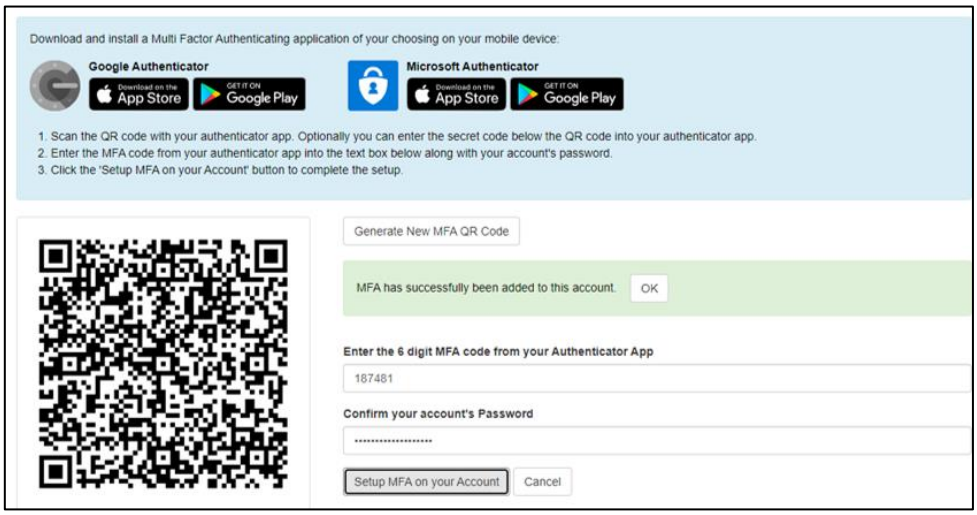

Figure 7 Confirmation MFA has been set up

i) Select ‘OK’.

Subsequent RMS Log-ins

On subsequent logons after entering your username and password you will need to enter a new security code obtained from the MFA app on your device to access the system.

a) Enter your email address and password

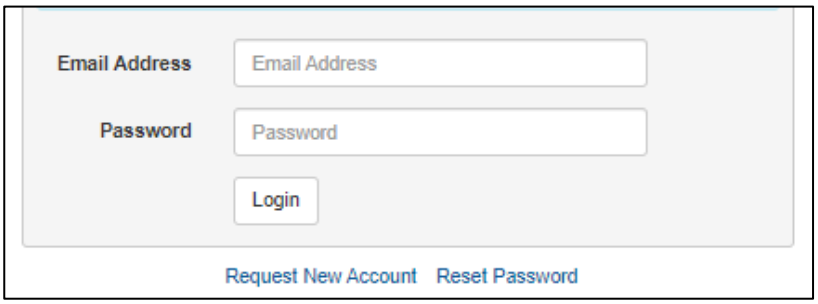

Figure 8 RMS Log in screen

b) Open the MFA authenticator app on your phone or device (a new code will generate every 30 seconds)
c) Enter the security code

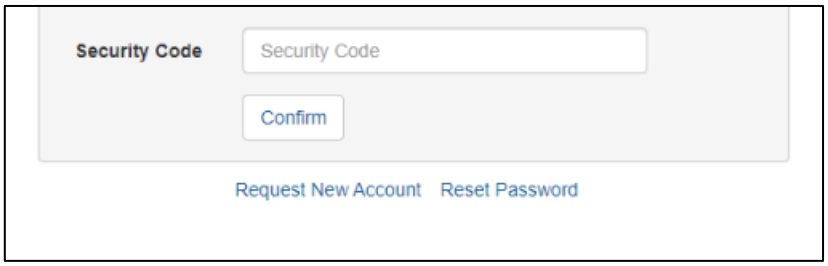

Figure 9 Security code screen

d) Click Confirm

e) The RMS Action Centre screen will now appear.