Guide for using Multi-Factor Authentication (MFA) when accessing the DER Register Installer Portal

To guard against misuse of the Distributed Energy Resources (DER) Register, AEMO is upgrading the login security protection.

In common with many other internet services (like Banks and government websites), AEMO is asking you to provide a second factor after you have logged-in with your account name and password.

You may choose one of three alternative methods of providing the second factor:

a) An authenticator app on your mobile phone that provides a time-based code (Recommended)
b) An SMS code sent to your mobile phone.
c) A phone call to your mobile phone or fixed-line phone

The Authenticator app is strongly recommended because it provides the most secure protection. The SMS and call options are provided for convenience during the initial period of activation. They will likely be discontinued in future.

These user notes provide information on how to setup and use MFA to access the DER Register Installer Portal. If you are registering as a user for the first time, you should begin by following the registration instructions contained in the Guide to DER Register Installer Portal (aemo.com.au).
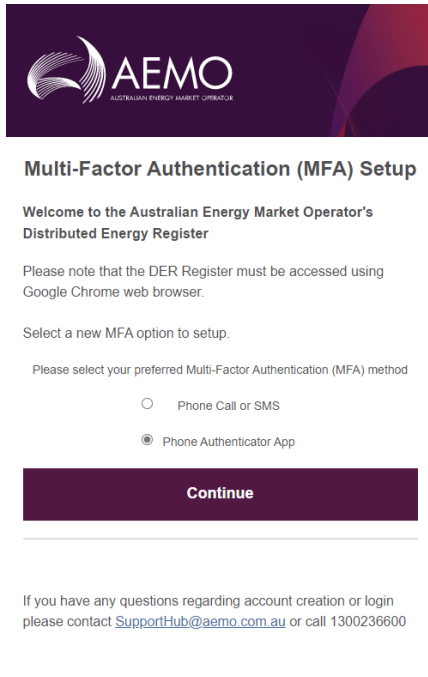
If you are existing user of the Portal, you may configure or reset your MFA setting at the MFA reset website: MFA RESET

1. Authenticator App

This is the most secure way of providing a second factor to prove your identity. You will install an application on your mobile phone that can generate a series of time-based one-time password (TOTP) codes unique to your phone. These codes will verify that you are the person logging in.
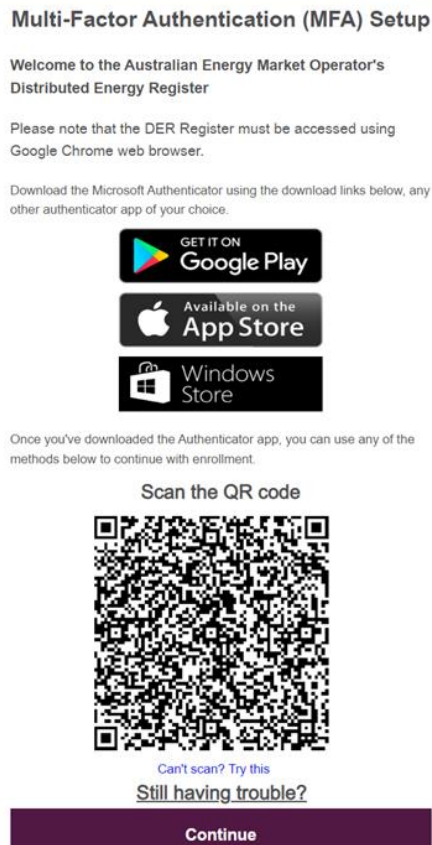
Follow these steps to configure your phone with the Authenticator App.

a) At the MFA setup screen select "**Phone Authenticator App**"
Then, press **Continue**.

b) The screen will display instructions and a QR code like this.

c) On your phone, go to your device's App store and download Microsoft Authenticator. If you already have another Authenticator App installed that follows the TOTP standard (e.g., Google Authenticator) then you may use that instead.

The instructions that follow are for Microsoft Authenticator.

d) In the App store, find the App and press **Install**
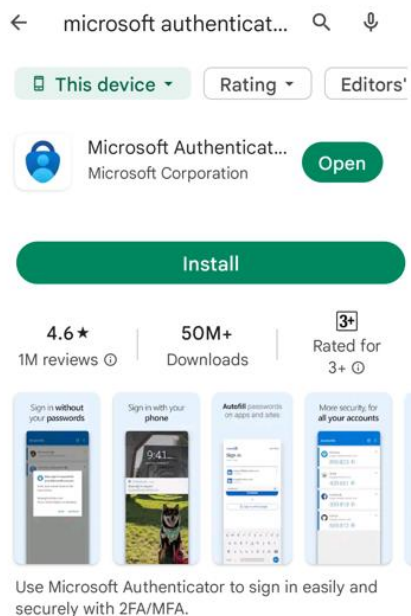
e) Open the app and press **+** (plus) to add an account
f) Press **Other account**
g) Use your phone's camera to read the QR code displayed
h) The Authenticator App will add your account
i) Select the new account and you will see the time-based password code. A new code will be generated every 30 seconds.
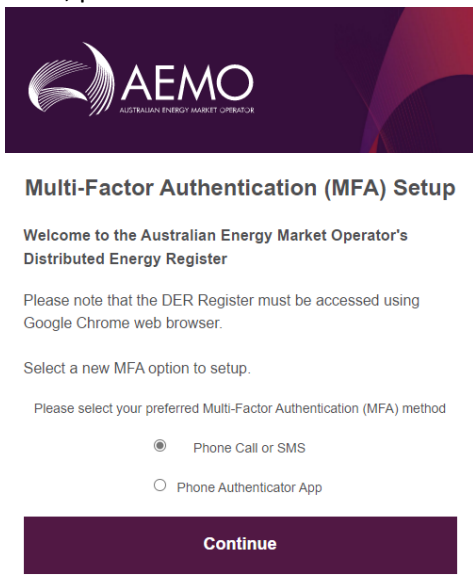j) Enter the code into the DER Register Verification screen, then press **Verify**
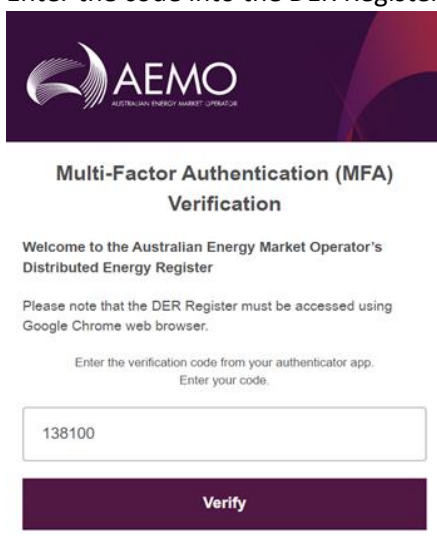
k) You are now verified and able to access the DER Register

2. SMS code sent to your Mobile Phone

This method is useful when you don't have a phone capable of running the Authenticator App

a) At the MFA setup screen select "**Phone**"
Then, press **Continue**.

b) Enter your **Country Code** and **Phone Number**, then press **Send Code**

c) After a short time, you will receive an SMS message on your mobile phone. Enter the password code into the DER Register verification page. Then, press **Verify Code**

d) You are verified and can proceed to use the DER Register

3. Receive a confirmation phone call at your mobile phone or fixed-line phone
This method is useful when you cannot receive SMS messages.

a) At the MFA setup screen select "**Phone**"
Then, press **Continue**.

b) Enter your **Country Code** and **Phone Number**, then press **Call Me**

c) After a short time, you will receive an automated phone call. Follow the instructions to verify your identity. You will then be able to proceed to use the DER Register.
(Note: The American expression "Pound Key" means the # key.)