SM MPI Two Factor Authentication

AEMO has introduced two factor authentication for logging into the System Management MPI due to the associated security risk of relying on single factor authentication (*User Id*/*Password* combination).

AEMO's preferred application for Two Factor authentication is Microsoft Authenticator which is available on the iOS and Android store.

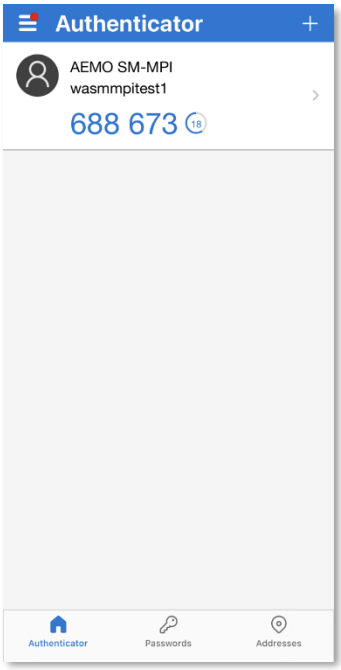
1. Log in

1. Following log on using the *User Id* and *Password*, if the end user has not logged into the MPI before (or registered for Two Factor Authentication), the end user will be presented with a QR code for scanning

Figure 1 QR Code Image

2. Scanning the QR Code as shown in Figure 1 using the Microsoft Authenticator application will add the account to the end user's device as seen in Figure 2.

Figure 2 Microsoft Authenticator setup for AEMO SM-MPI



3. Entering the code generated by the Microsoft Authenticator application for *AEMO SM-MPI* will log the end user into the System Management MPI.

SM MPI Two Factor Authentication

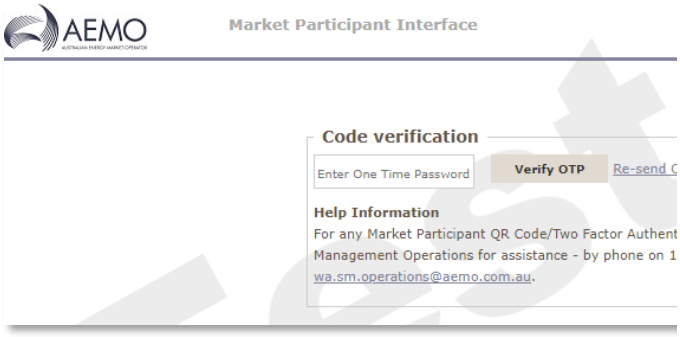
Figure 3 Two Factor Authentication code verification

2. Two Factor Authentication reset

1. If the original authenticator device is unavailable (e.g., new phone/device), clicking on "I don't have a verification code. Send me a One Time Password to my email instead" will send a One Time Password email to the User Id's associated email account for Two Factor Authentication reset.

   Note: If Microsoft Authenticator is already setup on the device for the SM MPI, for some devices you may need to remove the existing entry first. Otherwise, an error may occur when it attempts to overwrite the existing setup.

Figure 4 Two Factor Authentication reset



2. The end user will have three minutes to enter the One Time Password (under Figure 4). After such time, it will expire, and a new One Time Password will need to be requested by clicking on the "*Re-send One Time Password (OTP)*" URL.
3. Following successful Code verification of the One Time Password, the end user will be presented with a QR Code to scan using the Microsoft Authenticator application. See Figure 1 above.

3. FAQ's

Q: I do not have a user account to the SM MPI, how do go about getting access?
A: User accounts are created by the AEMO Support Hub and require the IT Contact within your organisation to request access. Please have your IT Contact speak to the AEMO Support Hub (1300 236 600 or by email at supporthub@aemo.com.au).

Q: Can I use Google Authenticator instead of Microsoft Authenticator?
A: Yes, Google Authenticator will also work, however Microsoft Authenticator is AEMO's preferred application for Two Factor Authentication.

Q: I did not receive my One Time Password by email after requesting it?
A: Check your junk mail folder or have your IT Contact speak to the AEMO Support Hub to verify the email account associated with the User Id you are using.

Q: I'm having trouble with the Two Factor Authentication process, who do I speak to?
A: WA System Management Operations (1300 989 797, Option 2 or wa.sm.operations@aemo.com.au) will handle queries in relation to Two Factor Authentication issues.

Q: I'm having trouble with my user account, who do I speak to?
A: AEMO Support Hub (1300 236 600 or by email at supporthub@aemo.com.au) will handle queries in relation to user accounts (your IT contact will need to speak to the AEMO Support Hub).

SM MPI Two Factor Authentication

Q: I've reset Two Factor Authentication and have tried setting it up again on the same device it was on previously and I am getting a warning message on my device?

A: This is expected behaviour. If Two Factor Authentication has been setup on the same device previously, you will need to overwrite the existing setup to continue. If overwriting fails, remove the existing entry for the SM MPI from Microsoft Authenticator first.