Application: SAFE ORM (External)

New Features

Ref ID	Application Area	Description
0001	Requestor login	Ability to enable MFA for requestor logins via a user selected mobile authentication app.

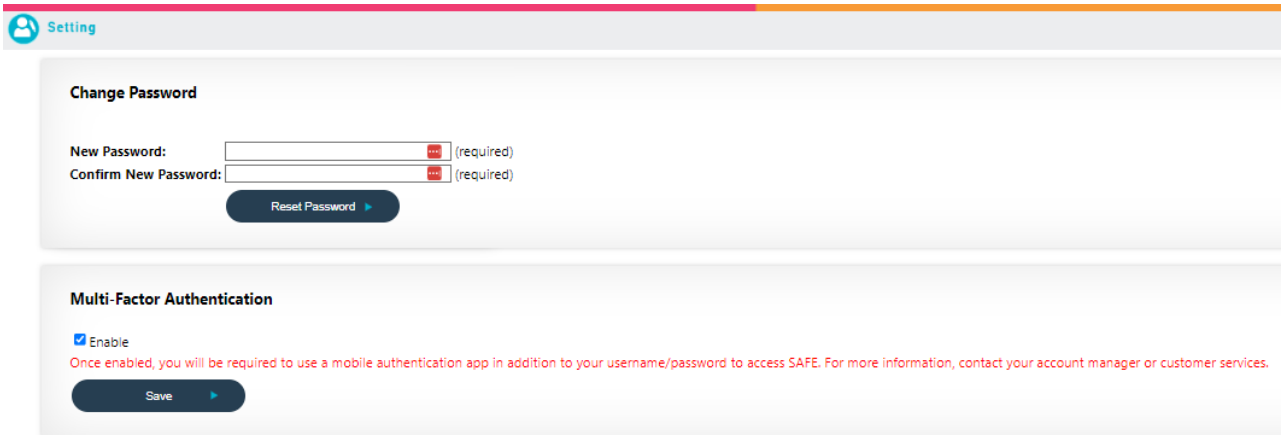
Detailed description:

To improve SAFE security posture and in response to customer requests, MFA (Multi-factor authentication) has been added as an **optional** setting for requestors.

Once enabled, on next login attempt, SAFE will require the user to register an authentication app using their mobile phone.

Once an authentication app has been registered, it will display a code which needs to be entered each time the user logs in.

The option to enable MFA is found under the settings page:

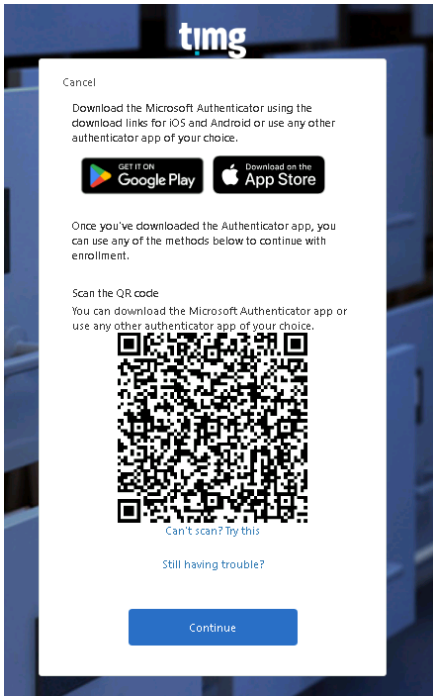


NOTE: For all users, the user login screen will now request users to enter a username/requestor ID first, and then a password. Followed by an MFA code if MFA is enabled.

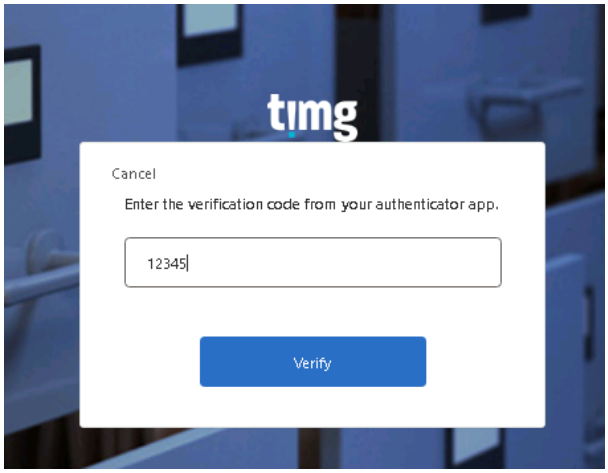
MFA Registration steps:

After enabling MFA for the requestor, on next login you need to follow these steps to register an authentication app:

1) Login using requestor ID and password as usual
2) The user will be presented with the below screen, instructing them to download an authenticator app of their choice, we recommend either Microsoft Authenticator, or Google Authenticator.



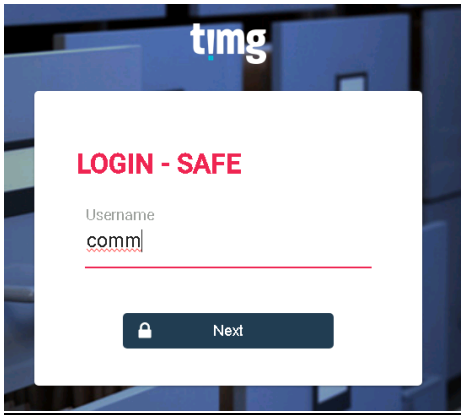
3) After downloading and opening an authenticator app, add a new service using the "+" icon and "Scan a QR Code"
4) Scan the QR code presented on SAFE with the mobile phone
5) A new code will be added to the authenticator app called "TIMG NZ - SAFE"
6) Click "Continue" in SAFE
7) Enter the code provided by the authenticator app as instructed below



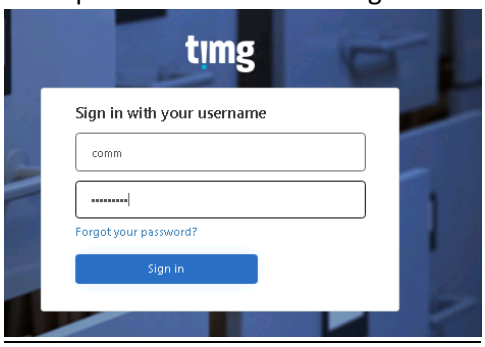
8) After correctly entering the verification code from the app, and clicking "Verify" the user will be logged in.
9) MFA setup complete

Login flow without MFA enabled:

1) Enter username/requestor ID and select “Next”



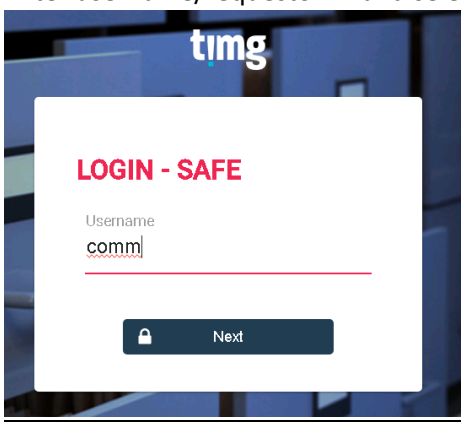
2) Enter password in the following screen and select “Sign in”



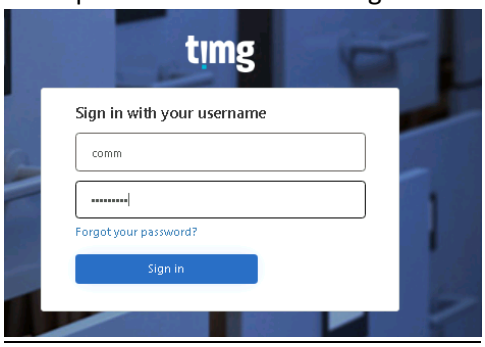
3) If the password is correct, the user will be logged in and land on the SAFE dashboard
4) Login complete

Login flow with MFA enabled:

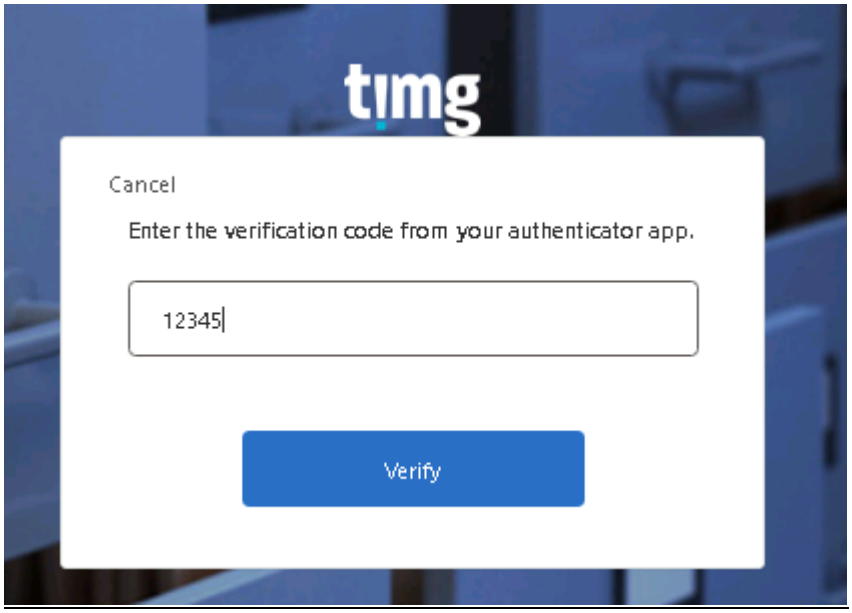
1) Enter username/requestor ID and select “Next”



2) Enter password in the following screen and select “Sign in”



3) Open the authentication app used during registration (see MFA registration steps above) and enter in the code for “TIMG - SAFE”. Click “Verify”



4) If the code entered was correct, the user will be logged in and land on the SAFE dashboard
5) Login Complete