



goAML EE Version 5.4_FIC

Web Two Authentication

June 2025

CONTENTS

1. OVERVIEW	3
2. AUTHENTICATING WITH 2FA.....	3
2.1. New User Setup.....	3
2.2. Log in	4
2.3. Lost Google Authenticator / Resetting the account.....	8

1. OVERVIEW

Two-factor authentication (2FA) enhances security by requiring an additional verification step to prevent unauthorised access to the application.

By default, authentication relies on a single-factor—the user enters their correct password associated with their username to gain access to the system. However, when 2FA is enabled, users must complete a second verification step before authentication is granted.

The goAML web application supports two methods for this second factor:

- Time-based one-time password (TOTP)
A six-digit code generated by the Google Authenticator app on the user's smartphone, which refreshes every 30 seconds.
- One-time password (OTP)
A code generated by the goAML web application and sent to the user's email. This code remains valid for a specified duration

2. AUTHENTICATING WITH 2FA


2.1. New User Setup

For OTP, no setup is required. The authentication code will be sent to the email address associated with the user's account.

For **TOTP**, users must install the Google Authenticator app on their smart device. The app is available for both Android and iOS platforms.

Upon approval, during a new user's first login, they will enter their username and password and then be presented with a QR code. This QR code must be scanned using the Google Authenticator app. Once scanned, the app will display an entry with the account title configured in the settings, along with a six-digit authentication code that refreshes every 30 seconds.

2.2. Log in



Please sign in with your username and password. If you do not have a username and password you have to register before logging in.

User Name


Password

LOGIN >>


Register Forgot Password Close

For **OTP**, after the user has entered their username and password an email with the one-time code will be sent to the user.

The **Use fallback authentication** link will only be shown if fallback authentication is configured as per the setting above. Clicking this link will send the **OTP** code via email and display the Login dialog above.



Scan the QR Code or enter the key below into your two factor authenticator app.



Key: GE4T ONZT G43T AAAA

[Use fallback authentication](#)


LOGIN >>

Register

Forgot Password

Close

The Login dialog will display an input field to enter the code and the time by which the user must login before the code becomes invalid, similar to the image below.



Please enter the verification code that has been emailed to you.
This code is valid until 12:35:44

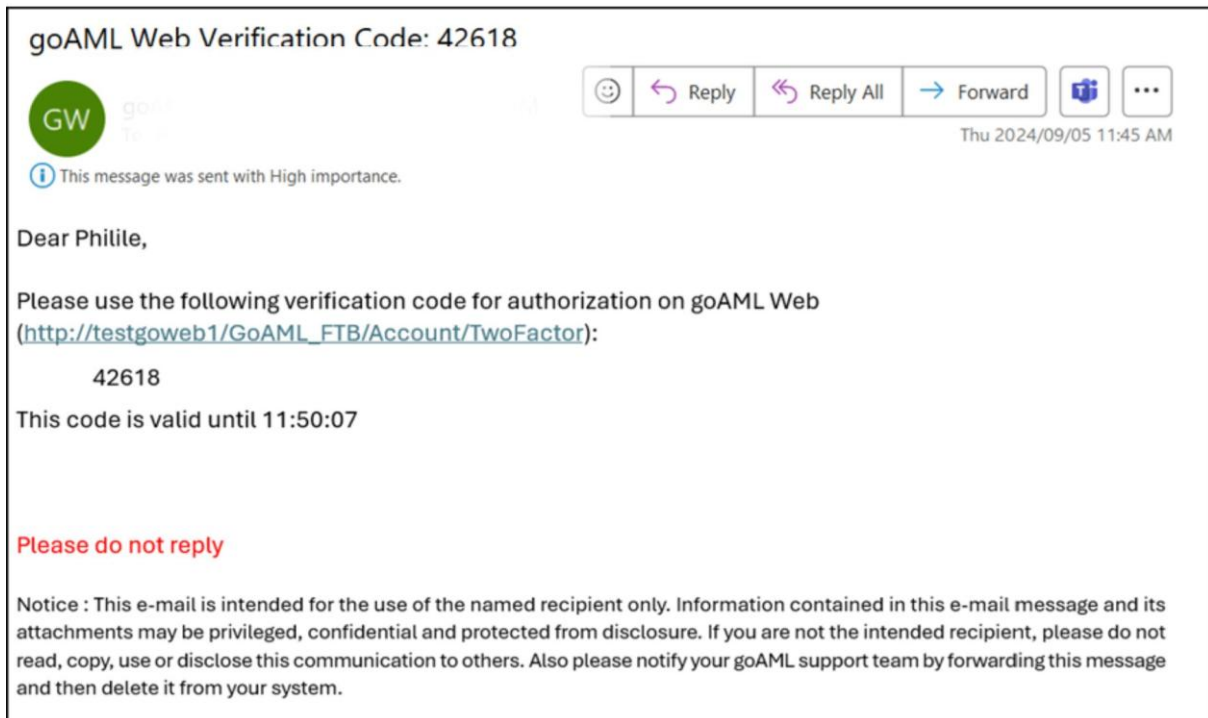
LOGIN >>

Register


Forgot Password

Close

Email example



For **TOTP**, after the user has entered their username and password. The Login dialog will display an input field to enter the code from the Google Authenticator, similar to the image below.



You login is protected with an authenticator app.
Enter your authenticator code for goAML Web
below.

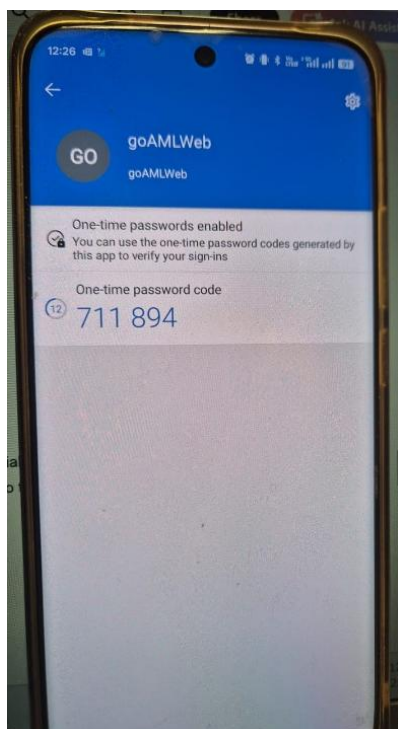
[Use fallback authentication](#)

LOGIN >>

[Register](#) [Forgot Password](#) [Close](#)

Google authenticator

The digital number changes after 30 seconds.

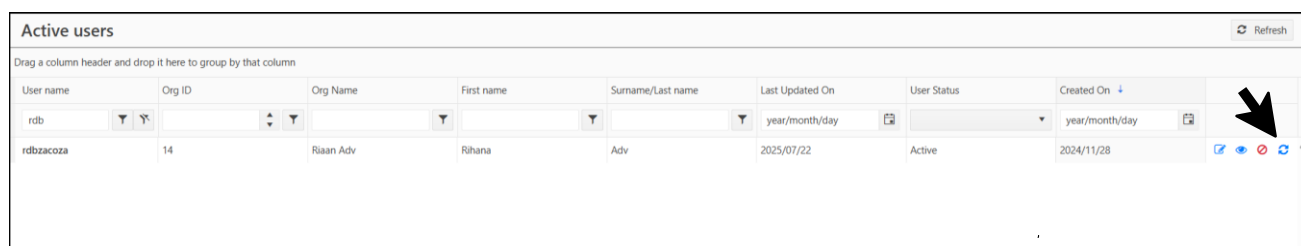



2.3. Lost Google Authenticator / Resetting the account

Once a Google Authenticator has been lost or the row deleted in the App, the user does not have the ability to reset it themselves or get another QR Code.

For security reasons, they must contact the FIC and request a reset, this allows the FIU to make any security checks as necessary and makes it harder for an attacker to gain access if they have compromised a user's email account.

To get another QR Code, the password for the user must be reset. Log in as an FIC Administrator, go to **Admin > Active Users** search for the user and select the password reset button as shown in the image below.



Active users								
Drag a column header and drop it here to group by that column								
User name	Org ID	Org Name	First name	Surname/Last name	Last Updated On	User Status	Created On	
rdb					year/month/day		year/month/day	
rdbzacoza	14	Riaan Adv	Rihana	Adv	2025/07/22	Active	2024/11/28	

The user will receive a link to reset the password in an email. Once they log in with this new password, they will be presented with a new QR Code. After scanning this code to add the app back into the Google Authenticator, the user may then log in and will be prompted to change their password before continuing to the site.