goAML EE V5.4
REGISTRATION USER GUIDE
USER (INDIVIDUAL)

29 August 2025

CONTENTS

Table of Figures

1. OBJECTIVE OF THIS GUIDELINE

The objective of this guideline is to define and outline the process when an individual reporter who is a natural person acquires user credentials on the goAML platform to report suspicious and unusual activity, transaction and/or series of transactions to the Centre in terms of section 29 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act), in their own personal capacity.

2. STANDARD DEFINITIONS

The guideline must be read in conjunction with the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (the FIC Act) and the Regulations for definitions of terms used in the guideline. In this guideline, unless the context indicates otherwise:

Individual reporter	Refers to a natural person who acquires user credentials in order to file a report in terms of Section 29 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), (FIC Act) in their own personal capacity.
Regulations	Refers to the Money Laundering and Terrorist Financing Control Regulations made in terms of section 77 of the FIC Act and promulgated in Government Notice 1595 of 20 December 2002 as amended.
goAML/goAML Web	Refers to the integrated software solution implemented by the FIC as its preferred ICT platform for registration, reporting, data collection, analysis, case management and secure communications required for the FIC's daily operational functions and requirements.

> **Important information to be taken into account when registering on the goAML system**
> - All fields with an asterisk (*) are mandatory and must be completed as part of the registration process
> - All registrations must be approved by the FIC prior to activation
> - Supporting documents such as an identity document (ID) must be attached as part of the registration applications to the FIC:
> - All First Letters must be in Caps:
> - Words typed in all caps are not allowed

3. INTRODUCTION

As South Africa's national centre for the gathering and analysis of financial regulatory data, the role of the Financial Intelligence Centre (FIC) is to safeguard the integrity of the country's financial system and its institutions. In pursuit of this, the FIC Act mandates the FIC to identify the proceeds of crime, combat money laundering and the financing of terrorism, and facilitate effective supervision and enforcement of the Act.

Under this legislation, financial and non-financial institutions are required to fulfil certain compliance obligations, including filing of regulatory reports to the FIC. The information provided in these reports form the basis upon which analysis is conducted to develop financial intelligence reports for use by a wide range of law enforcement agencies and other government institutions to facilitate the administration and enforcement of the laws of the Republic. The FIC Act also sets out the enforcement and penalty regime for non-compliance with the FIC Act.

The FIC has implemented an integrated software solution as its preferred platform for registration, reporting, data collection, analysis, case management, and secure communications to its daily operational functions and requirements. In terms of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), reporting entities are required to register with the FIC.

Persons (individual reporters) wishing to file a suspicious or unusual transaction report with the FIC electronically in terms of section 29 of the FIC Act must obtain user credentials on the goAML platform in order to file the report in the prescribed manner.

4. goAML EE WEB

The link to access goAML EE is goAML.

When a user enters the URL into their web browser, the goAML EE homepage will open.

The landing page features these main options: **Register**, **Report**, and **Contact** information. To get started, first-time users need to register by selecting the **Register** button as illustrated in figure 1.
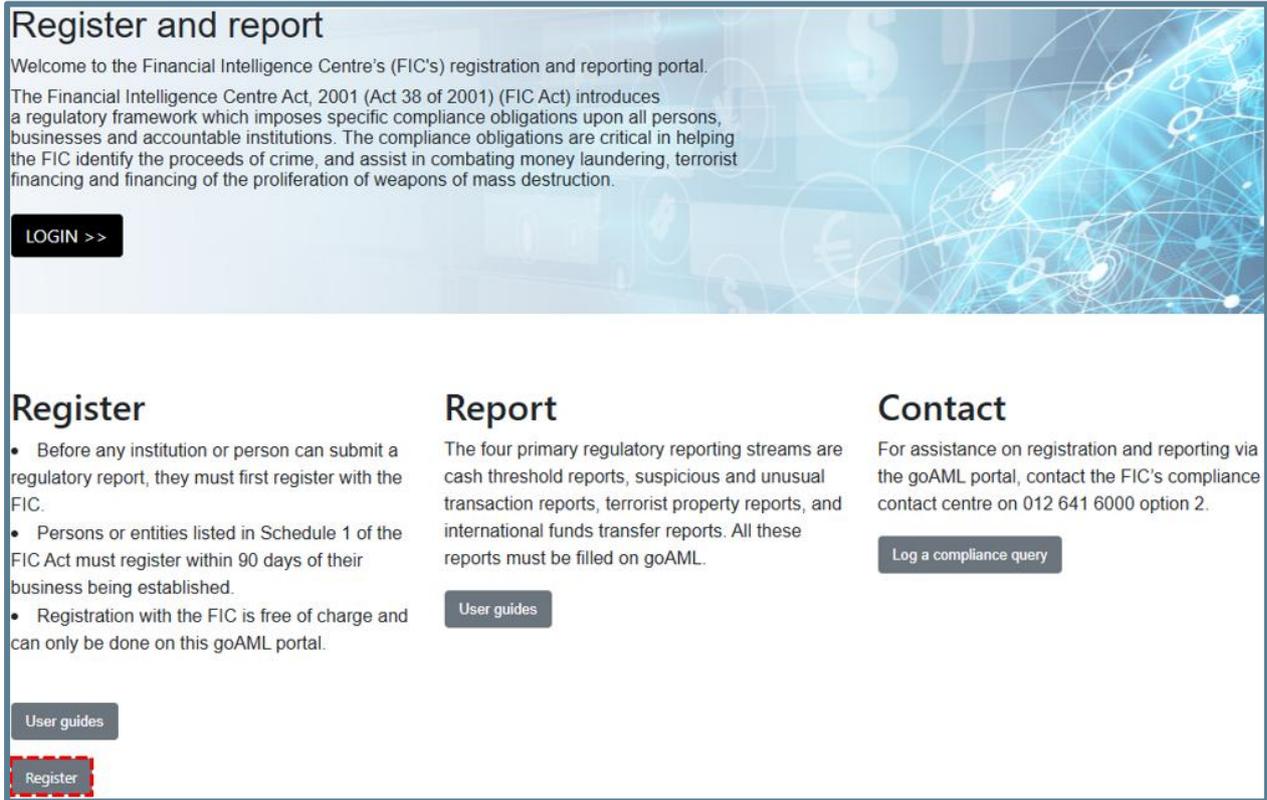
5. goAML LANDING PAGE

Figure 1: goAML landing page

The user (individual) must register by clicking the **register** button located at the bottom left of the page as illustrated in figure 1.
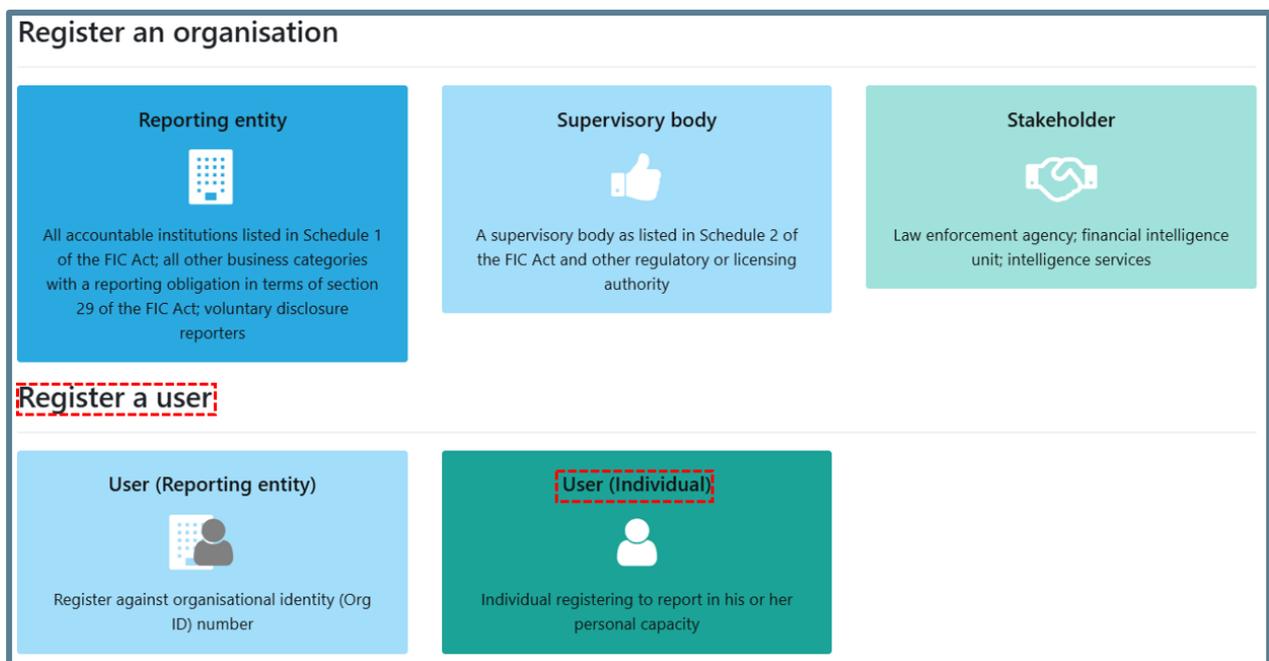
6. goAML REGISTRATION TILES

Figure 2: goAML registration tiles

> **Note:**
> - South Africa will be preselected in the 'country fields'; users can modify their selection by using the drop-down menu
> - The person e-mail address must be valid as it will be used for the login validation code delivery and official correspondence with the organisation
> - All fields marked with an asterisk (*) are required to be completed before submitting the registration form
> - FIC's mandate is to analyse and develop intelligence reports pertaining to financial crime in the Financial and DNFBP sectors, and the FIC is not mandated to analyse or refer disputes of a personal nature.

Registration tiles contain the '**Register an organisation'** and '**Register a user'** sections.

- All users are required to register on the goAML platform before submitting the report.
- A copy of the user's certified identity document and or authorisation letter must be attached and submitted to the FIC for approval in order to gain access to goAML.

7. INDIVIDUAL USER REGISTRATION ON goAML

Reporters that are required to submit reports must register to acquire access to goAML. The registration details of the user must be provided in this section. This section registers the individual user on the goAML system. To register the user, click the '**User (Individual)'** tile in figure 2, The registration screen will be loaded and display as illustrated in figure 3.

Figure 3: Registering User (Individual) fields

The user must complete all the required fields. Once all tabs are completed, the *red bar* on the left will turn green, enabling the user to submit the registration.

7.1. User (Individual) details

- Title: Title of the individual user

- First Name: First name of the individual user

- Surname: Surname of the individual user

- Gender: Gender of the Individual user

- Occupation: Official job title of the individual user

- Birth date: The date of birth of the individual user

- RSA ID: 13-digit South African ID Number (e.g. 9902251109876)

- RSA passport number: South African passport number

- Nationality: The status of belonging to a particular nation, whether by birth or naturalisation (If nationality is SA, RSA ID field becomes mandatory. If non-RSA nationality, complete the passport/foreign ID/permit number/refugee number/Asylum seeker field)

- Issuing Country: Country where non-South African passport/identity document was issued

- E-mail: Official e-mail address of the individual user

- Username: A unique identifier used to access the system

- Password: A secure login credential between 5 to 10 characters long, combining uppercase and lowercase letters, numbers, and special symbols.

- Confirm Password: Type your password again for confirmation

7.1.1. Address

- Type: The individual user's address. This can be business, physical or a postal address.

- Address: This is the location details specifying where the user resides

- City: The name of the city where the user resides

- Province/State: The name of the province where the user resides

- Country: The name of the country where the user resides

- Postal/Zip: The postal code of the town/city where the user resides

7.1.2. Phones

- Contact type: The preferred method of communication for reaching the user

- Comm.type: The preferred method of communication

- Country prefix: This is the international dialling code of a country e.g +27

- Number: The preferred contact number to be used. Numeric, digits (e.g. 0126416000)

7.2. Attachments

This section requires the user to attach a copy of the ID and/or an authorisation letter. To add documents, click the attachment tab. The next screen will appear as shown in figure 4

Figure 4: Attachment screen

To upload a document, click on "**Select files"** or "**drop files here to upload**" options.

Select the document to attach from the desired location and click '**Open'**.

The document will be attached under the **'Attachments'** tab.

7.3. Preview and submit

Once all the required details are provided, the **'Preview and submit'** tab will turn green, to enable the user to review and submit the form as illustrated in figure 5

Figure 5: Form preview

To finalise your registration, click the '**Preview and submit'** tab**.** A final confirmation screen will appear, indicated by a green bar on the left, confirming that all required information has been completed.

Figure 6: goAML registration final screen

Enter the verification code shown in the **Preview and submit** section into the designated code field. Then, click '**Submit user'** button to complete the registration, or select '**Cancel'** to withdraw the process. Once the registration form has been submitted, the pop-up screen will display with the **SHREG** reference number. A notification e-mail with the **SHREG** refence number will be sent to the registering user's e-mail address entered during the registration process.

Registration info has been submitted

Please wait for notification of acceptance/rejection by e-mail. Your request has been given the following reference number:

SHREG-250410-0000001

Figure 7: Registration confirmation

> Note:
> - When the FIC is satisfied with the captured registration details and attached documents, the user will be notified by e-mail about the acceptance of the registration.
> - When the FIC is not satisfied with the captured registration details and attached documents, the user will be notified by e-mail about the rejected registration.
>
> **Registrations will be rejected on goAML for the following reasons:**
> - If the user provides incomplete or inaccurate information on the system whilst registering
> - If the user provided incomplete registration forms, or complete the forms with inaccurate information
> - No verification documents are attached for registration

8. LOGGING ONTO goAML WEB

Once registration is approved, the user will gain access to the system by using the username and password created during registration. A second authentication will always be required before gaining access to goAML.

- **Step 1**: Download the Microsoft/Google Authenticator application on your mobile device
- **Step 2**: Click on goAML login page
- **Step 3**: Enter your username and password in the standard format captured during registration and click on **'LOGIN'**.
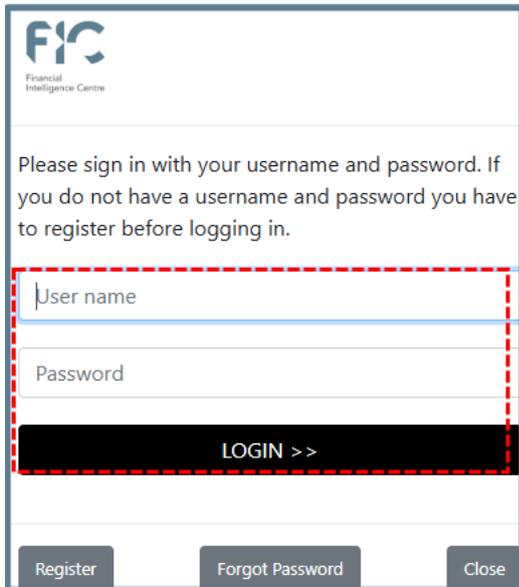
Figure 8: Login page

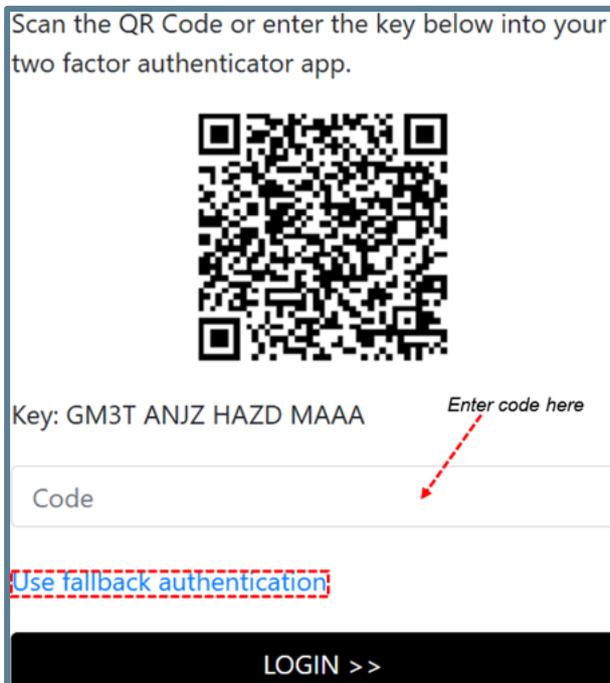A QR code authentication page will be displayed as shown in figure 10.

Figure 9: QR Authentication page

- **Step 4 (Option 1)**: Open the authenticator app on your mobile device and scan the QR code

- **Step 5**: Enter the time-based code displayed from the goAML shortcut in the code field

- **(Option 2): Or use fallback authentication:** Click on 'Use fall back authentication' option in figure 10 to receive a code via e-mail >enter the code and login.

Please note that the code remains valid for five minutes. Once the time elapses, select 'Use fallback authentication' to generate a new code.
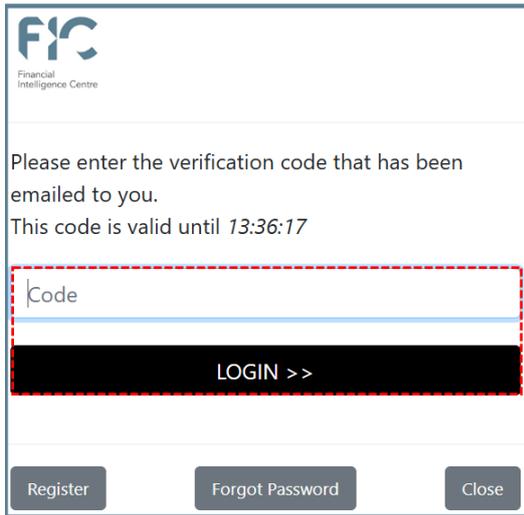
Figure 10: Authentication screen

9. UPDATING USER DETAILS OR ACCOUNT DETAILS

9.1. Change password

Figure 11: goAML landing page

The goAML system gives users the ability to update details, including password, user details, and org details.

- On the goAML landing page, hover the mouse curser over the username (**JMMJ**) and select **'Change Password'** as illustrated in figure 11. This will open the Change Password dialog box, where users can enter their current password, set a new password, and confirm the new password as illustrated in figure 12

Figure 12: Change password dialog

9.2. My user details

On the goAML landing page, hover the mouse curser over the username (**JMMJ**) and select **'My user details'** as illustrated in figure 11. This will open the **user details** form, where users can update the details and submit request as illustrated in figure 13.

Figure 13: User details

Once the request is submitted, the request window will display with the SHREG number as illustrated below in figure 14.

Figure 14: User details request page

The changes must go through three stages: **verification, approval, and finalization**. Once the request is finalized, a confirmation message containing the **SHREG** number will appear on the screen and will also be sent to the user's email address used during registration.

Figure 15: Confirmation page