Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

Federal Office of Police fedpol
Crime Prevention and Law
Money Laundering Reporting Office MROS

goAML Web-Manual

Registration & User Profile Management & MessageBoard

Version 1.0

1 Version Control

Version	When	What	Who
1.0	13.06.2024	Creation of first version	MROS

2 Table of contents

3 Introduction

The goAML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units (FIUs) and is one of UNODC's – United Nations Office on Drugs and Crime - strategic responses to financial crime, including money laundering and terrorist financing. goAML is specifically designed to meet the data collection, workflow management, analytical and statistical needs of FIUs.

FIUs play a key role in the fight against money laundering and terrorist financing as they are the central reception point for receiving, processing and analysing reports compiled by reporting entities[1] in compliance with their country's anti-money laundering and counter- terrorist financing legislation.

This document aims to give reporting entities an overview of the goAML IT architecture and to provide guidance regarding registration and goAML user administration. For information on how to enter or filing a report, please consult the goAML Web User manual, available on the webpage of fedpol in four languages.

4 goAML IT Architecture

The goAML system consists of two applications:

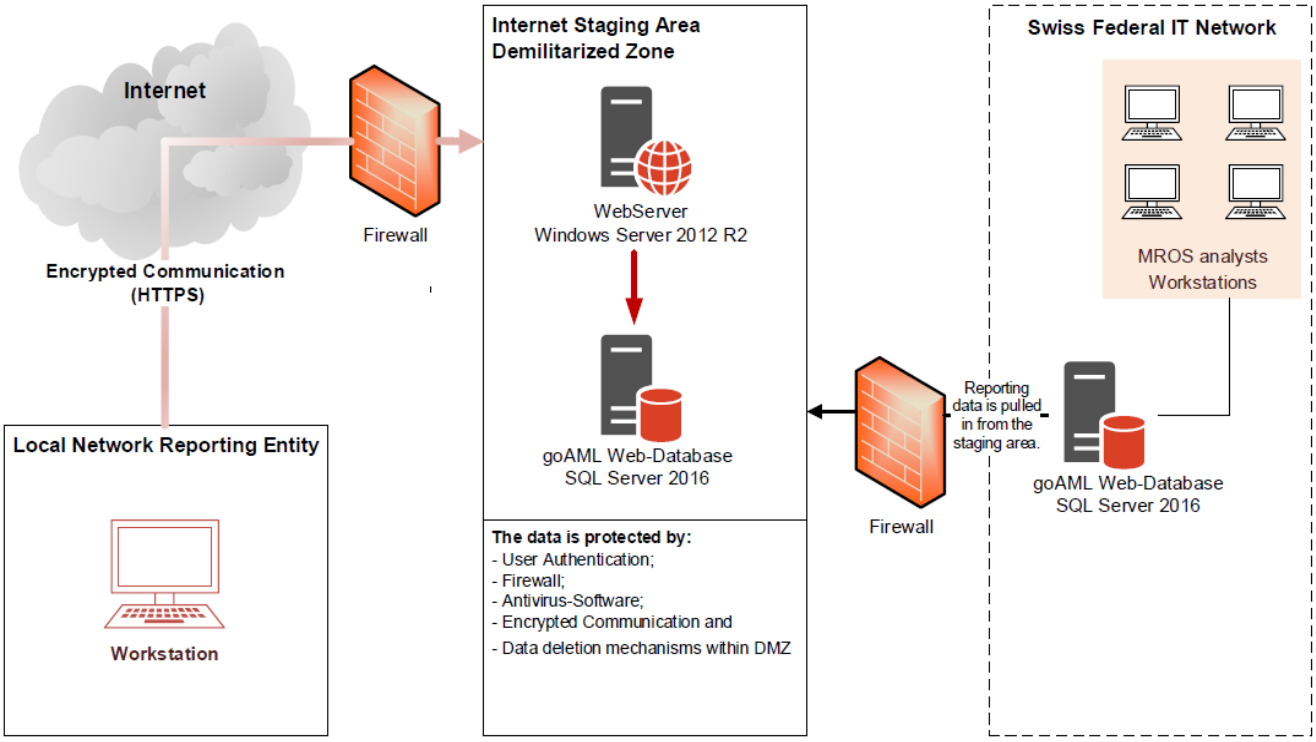
- the **external Web application**, which is accessible to all reporting entities, and
- the **internal MROS main application** (so-called client application), which is accessible to MROS personnel only. This is not covered by this manual.

The external goAML Web application provides a secure web-based interface between MROS and the reporting entities. Its main purpose is to provide a platform of communication between the FIU and the reporting entities, allowing the submission of reports and other information to MROS by **XML file upload** or by **filling in manually** the online reporting forms. Semi-automated reporting is also available as a third option, i.e. a combination of manual entry and uploading of the relevant transactions in XML format.

IMPORTANT: It should be noted that the information submitted is held in Switzerland and that **UNODC does not have access** to the data processed and stored within the goAML system. The following picture gives an overview of the goAML IT architecture applied in Switzerland.

[1] The term reporting entity is applied throughout this document and is a standard within goAML to define any financial intermediary or merchant authorised to submit suspicious activity reports in Switzerland based on the Anti-Money Laundering Act (AMLA) or Penal Code.

The following graph provides an overview of the goAML IT structure used in Switzerland:



goAML provides the option of submitting reports as XML files. XML is an IT language used to structure complex sets of data, such as suspicious activity reports.

When a report is being compiled manually via web form, the data is transferred via secure HTTPS internet connection to the DMZ (demilitarized zone). The DMZ is located outside the Swiss Federal IT Network and corresponds to a secure IT environment.

In the DMZ the data is protected by the following data security measures:

- firewall;
- encrypted communication;
- two-factor user authentication measures (2FA);
- antivirus software;
- data deletion mechanisms within DMZ.

If, for example, a reporting entity takes several days to finish its manual report compilation process and, while working during those days, saves the preliminary data set in the goAML form, this data set is stored in the DMZ and is therefore protected by the security measures mentioned above.[2] If the reporting entity decides to upload the data via automated XML file, this data is stored temporarily in the DMZ as well.

[2] Despite this high protection level, in order to minimize any potential data risk, it is advisable to finish the manual report compilation process and its submission to MROS in the shortest possible time frame.

Once the report has been completed and submitted to MROS, its content is then validated by the goAML Web application to check whether it complies with the data structure defined by MROS.

If the data validation checks are successful, the data set remains on the goAML web database server within the DMZ until it is permanently deleted by the deletion process illustrated in chapter Automated deletion terms for reports and data within goAML Web. A pull mechanism ensures that the data is uploaded timely into the Swiss Federal IT Network, which is protected by enhanced Swiss Federal IT security guidelines.

In a scenario where the data validation checks are not successful, meaning the report submitted by the reporting entity is not complete or incorrect, this data set is automatically routed back by the goAML Web application to the reporting entity. The reporting entity then receives an automated email from the system (sent by: goAML Workflow [mailto:goamlVALIDATION@fedpol.admin.ch]) explaining the reason(s) for rejection, without any client data. This allows the reporting entity to correct the report and resubmit it to MROS. Once the data is resubmitted, the process explained above starts again.

5 Field labelling syntax

The following syntax applies in the goAML system and aims to further specify the label of the corresponding field in the goAML Web application as follows:

Syntax	Explanation
{word}*	The asterisk after a word means that this particular field must be filled in mandatorily, otherwise the report will not be accepted for submission.
Inactive (n/a)	All fields marked with 'Inactive (n/a)' have been technically blocked by MROS to prevent any data being entered. If the reporting entity wishes to submit information for which there is no adequate place in goAML, please contact MROS to agree on the most suitable solution.
	This symbol indicates that a separate section is accessible. To do so, the user selects the '+' sign and a new screen with additional fields opens up.

6 Registration

To guarantee maximum security, a two-factor authentication will be required for users to log in to the system. With this functionality, a code sent via SMS is required in addition to the user name (Login ID) and password for a successful login to the system. The two-factor user authentication is explained in detail below.

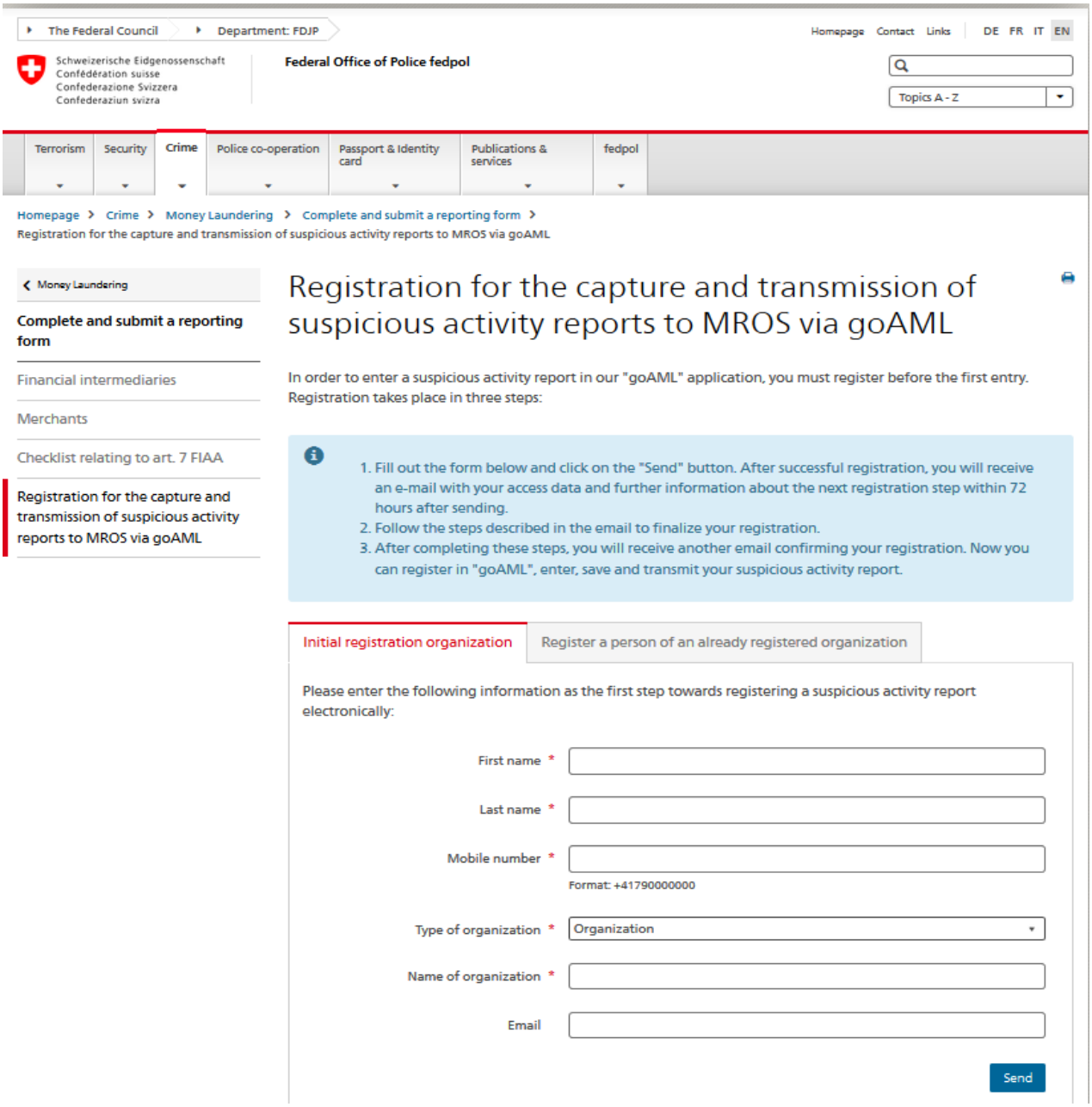
Please note: The first person who registers on behalf of an entity is automatically assigned administrator rights on behalf of that entity and, for example, is also to approve any user access requests submitted on behalf of the reporting entity it represents. The administrator role can be changed later by the current administrator, however, in the interest of efficiency, an appropriate person should be the first to register as an administrator on behalf of the entity.

6.1 Registering as a new Reporting Entity

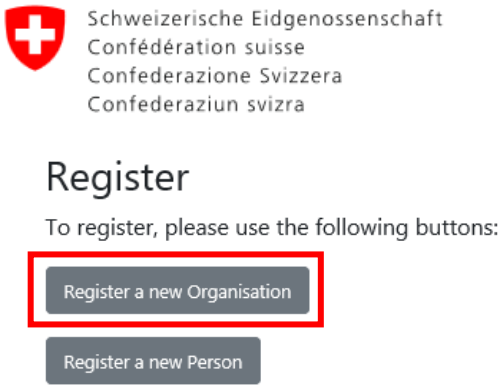
All reporting entities must first register with MROS and in a second step set up a goAML user account before they can fully access goAML Web. This section provides guidance on how to do so:

- The link below will take you to a registration form (see image on next page). Please follow the instructions and enter the required information in the relevant fields:

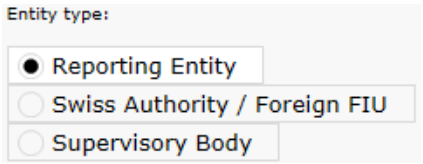
https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/meldung.html



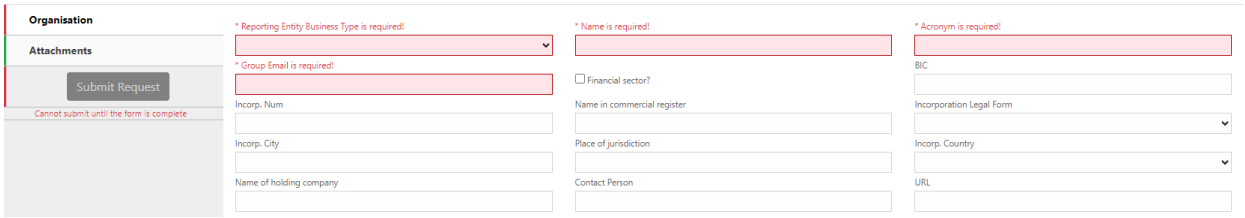
- As soon as you have entered all the information and sent the form, MROS will receive notification. It will then check your details and carry out the next steps for registration in the SSO portal.
- Within 72 hours of submitting the registration form, if your registration is successful, you will receive an email with your access details and further information on the next stage of the registration process.
- Follow the steps described in the email so your registration can be finalised.
- Once all these steps are complete, you will receive an email confirming your registration. You can now log in to goAML, and enter, save and transmit your suspicious activity report. You can also amend your details.
- Access the entry portal for the goAML Web application as explained in chapter 7 ‘The entry portal of the goAML Web application’ and select ‘Register a new Organisation’:



- At the top select 'Reporting Entity', 'Swiss Authority / Foreign FIU' or 'Supervisory Body' depending on the type of organisation attempting to register in goAML. In order to decide which category your organisation belongs to, please use the definitions explained in the glossary at the end of this document.



- Fill in the fields of the form with your organisation's data. Selected fields are to be completed by using the drop-down arrow and then selecting the most appropriate category:



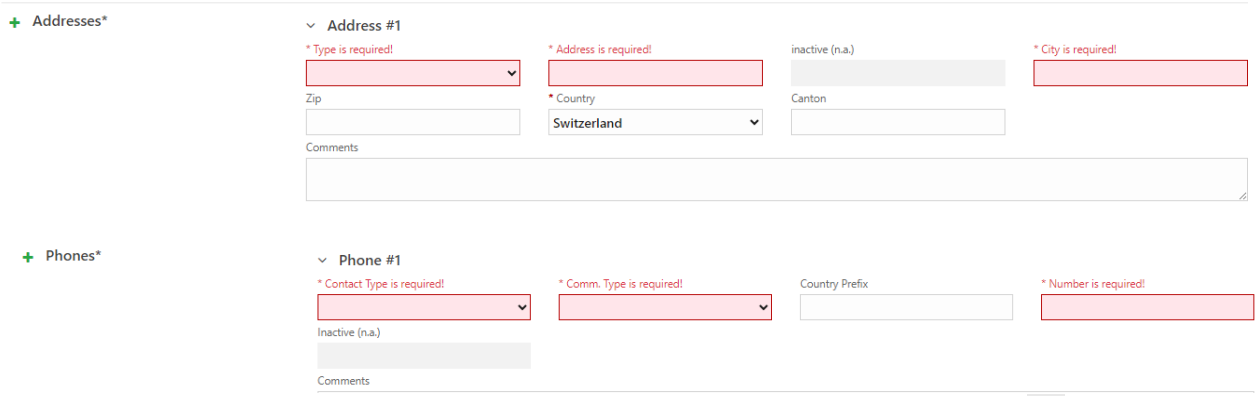
- **Please note**: the field 'BIC' is **only addressed to banks** and is to be filled in by them mandatorily with the requested information. **Non-banks** are kindly asked to select just **No** in the field '***Financial sector?***' above, which allows them to skip the field 'BIC'.

- **'Group Email' field**: Notification emails informing that there is an unread item on the message board or notifications related to entity change requests will be sent to this group email address. Considering these types of notifications are not meant to be for individuals, this field must contain a group email address. This address is therefore different from the one entered for the user (see chapter 'Message Board' for additional details).

- **'Reporting Entity Business Type' field:** Banks are requested to select the applicable bank category in the 'Reporting Entity Business Type' field according to the official *List of reporting banks in Switzerland* compiled by the Swiss National Bank SNB (e.g. regional and savings banks, foreign-controlled banks) the first time they register in goAML. The respective list can be accessed from the SNB website at the following link: here.

- The system also requires the entity's phone number and physical address. It is mandatory to provide this information so that MROS can contact the reporting entity**.** To access these fields, click on the adress section:

-



Please note that after adding the first phone number or address the sign on the left is still active, meaning the user can add multiple phone numbers or addresses:

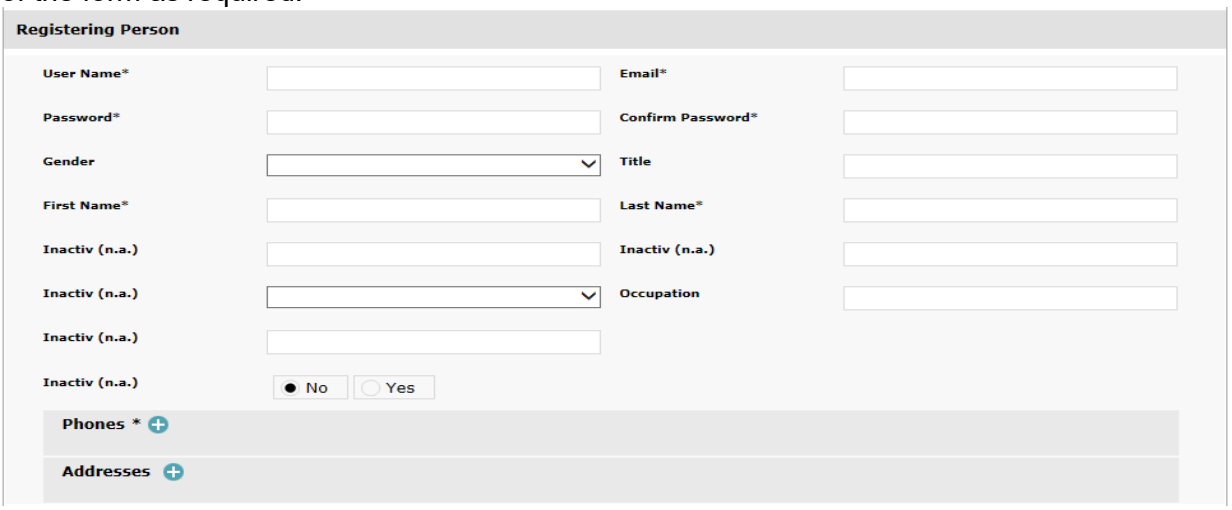
Should the user want to delete a data set, please select the garbage-sign on the right of the screen.

- **Once all entities fields have been completed, the registering person will have to request access (see next chapter).**

6.2 Registering an initial user

Reporting entities should note that the first person who registers on behalf of that entity will automatically be assigned administrator rights on behalf of the entity. Administrator permissions can be transferred to someone else from the same reporting entity later, however, in the interest of efficiency, it is recommended that an appropriate person be the first person to register on behalf of the entity.

- Continue by scrolling down on the same screen illustrated in chapter 6.1 and fill in the fields of the form as required:



- **User Name** field: The User Name is specified by the upstream security system and cannot be changed.
- **Email** field: The personal email address of users in the process of registering is passed on by the upstream security system and cannot be changed. The acceptance notice of the registration will be sent to this address (see chapter 14 ‘Message Board’ for additional details).

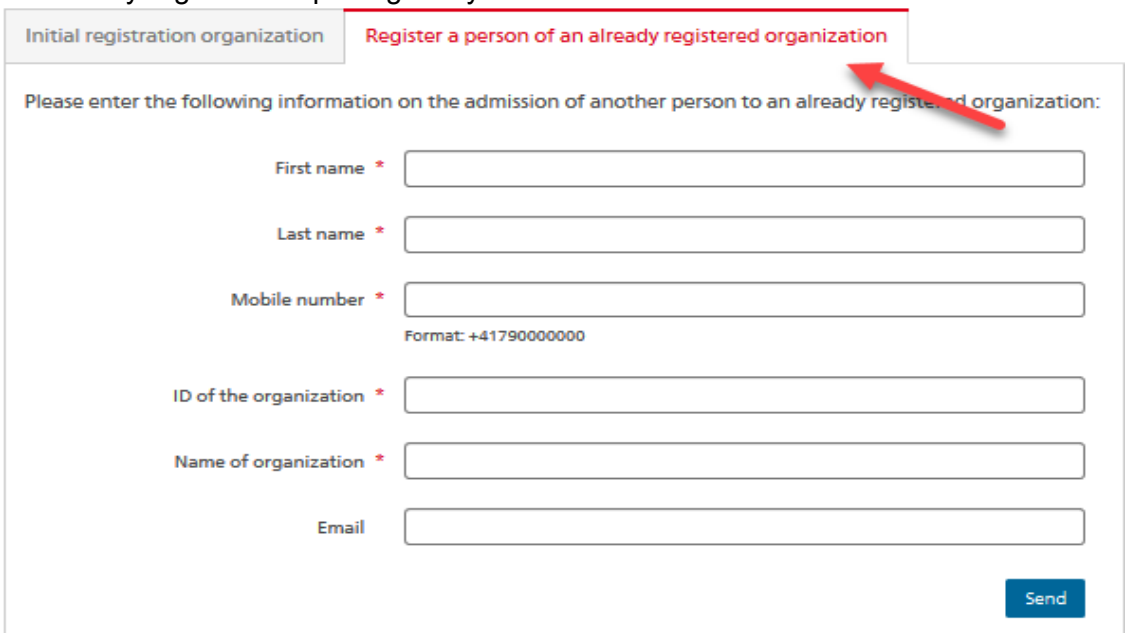
- **Password** field: the password is specified by the upstream security system and cannot be changed.
- **First Name** and **Last Name** fields: These fields are required by the system. However, if the registering person does not want to disclose their first and last name to MROS, an alias name may be used instead (e.g. first name = United; last name = Bank).
- **Phones** section: This is the place where the registering person **must** fill in their **direct** phone number. This information is mandatory. Once a suspicious activity report has been submitted, this phone number allows MROS to contact the relevant person in case of questions.
- MROS does not require any attachments for the registration process.
- Once all data is completed, enter the security code (captcha) displayed on the screen into the field at the bottom of the form and select Submit Request:

The captcha ensures that you are not a robot. If the entry is incorrect, the registrations process is aborted.

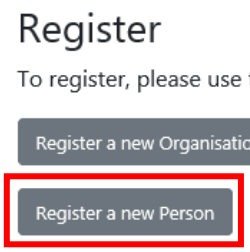
- The registering person will now receive an automated email notification from goAMLWeb Workflow (goamlVALIDATION@fedpol.admin.ch) with a reference number. It is advisable to save this email (at least temporarily) in case there are any problems with the registration.
- As soon as the registration request has been approved by MROS, the registering person will receive another automated confirmation email from MROS.

6.3 Registering as a new Person for an existing Reporting Entity

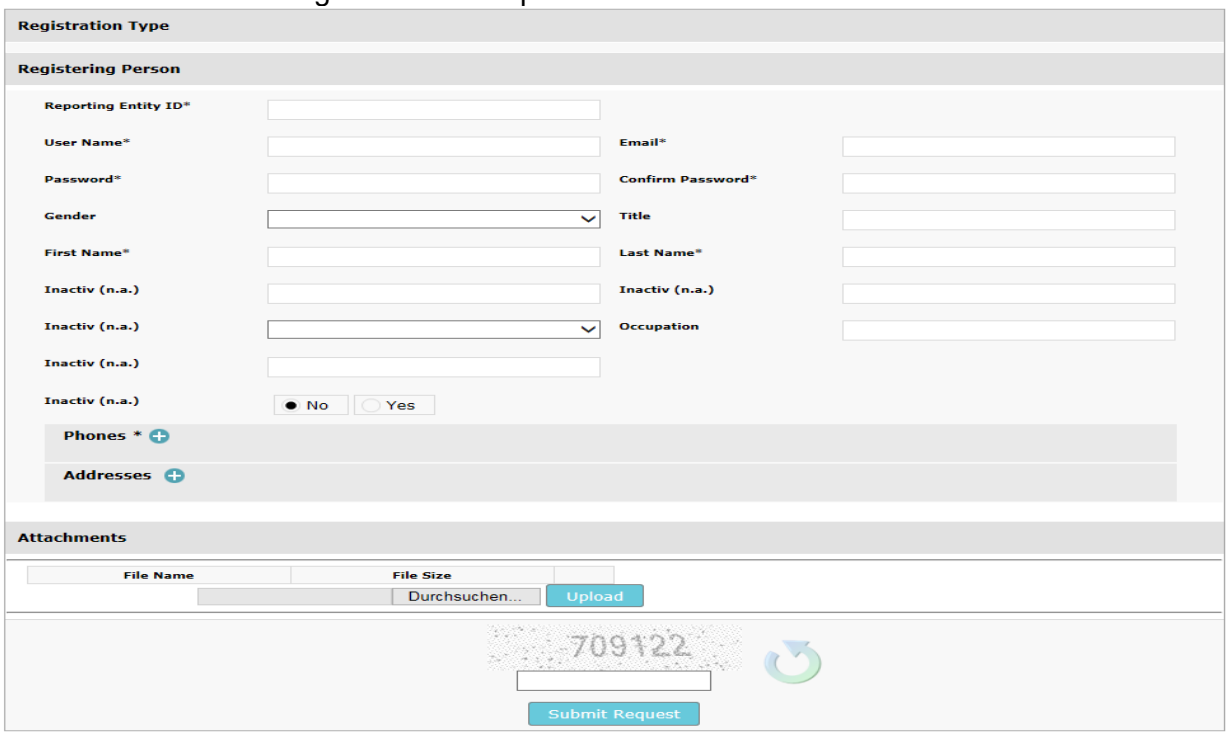
If a reporting entity **is already registered** in goAML and additional users working for this entity are to be registered, the procedure to follow is set out under point 6.1. A new person can be added to an already registered reporting entity in another tab:



- Access the entry portal for the goAML Web application as explained in chapter 'The entry portal of the goAML Web application' and select 'Register a new Person':



- The following input screen is loaded:



- **Reporting Entity ID** field: Enter the entity reference number assigned to your organisation by goAML at the time the entity was registered in the system according to chapters 7.1 and 7.2.
- **User Name** field: The User Name is specified by the upstream security system and cannot be changed.
- **Email** field: The email address is passed on by the upstream security system and cannot be changed.
- **First Name** and **Last Name** fields: These fields are required by the system. However, if the registering person does not want to disclose his/her first and last name to MROS, an alias name may be used instead (e.g. first name = United; last name = Bank).
- **Phones** section: This is the place where the registering person **must** fill in a **direct mobile** phone number. This information is mandatory. Once a suspicious activity report has been submitted, this phone number allows MROS to contact the relevant person in case of questions.
- For an explanation of the remaining registration fields and steps, please refer to the explanations provided above.

Note: goAML administrators of a reporting entity are **required** to approve goAML access requests submitted by new users of the same reporting entity (under the tab -> Administration -> User Requests).

6.4 Deactivation of a user account due to inactivity

If a user account is not used for longer than six months, it is automatically deactivated for security reasons. In such cases, the users concerned should contact fedpol via goaml.info@fedpol.admin.ch so their account can be reactivated.

7 The entry portal of the goAML Web application

The *goAML* Web application can be accessed via the following link: https://www.goaml.fedpol.admin.ch.

As goAML requires two-factor authentication (2FA), when accessing the above website, the SSO portal page appears first:

After entering the Login ID, password and the code received via SMS, the user is automatically directed to the goAML homepage:

Once the user has clicked one of the following buttons

- Login
- Register a new Organisation
- Register a new Person

the desired language (in abbreviations: EN, DE, FR or IT) can be selected in the top right-hand corner of the system interface that appears.

All published goAML documents (including information on when they were last updated) are available on the entry portal, as well as details on how to contact MROS.

8 Login and Logut

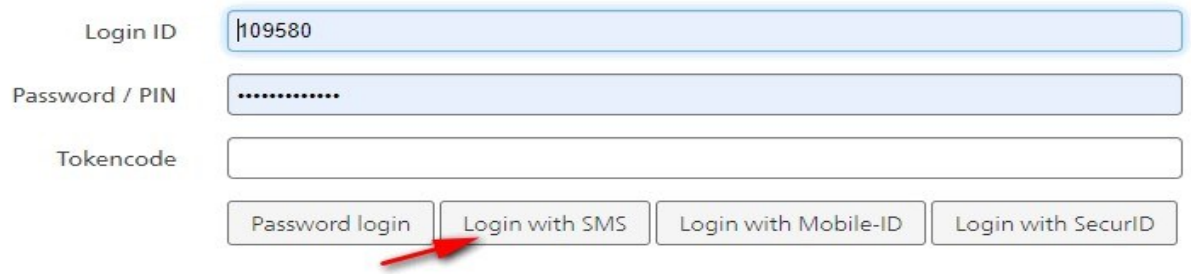
8.1 Logging in to goAML Web

To log in to goAML Web, the user needs to be registered and their access request (as detailed in the previous sections) must have been approved.

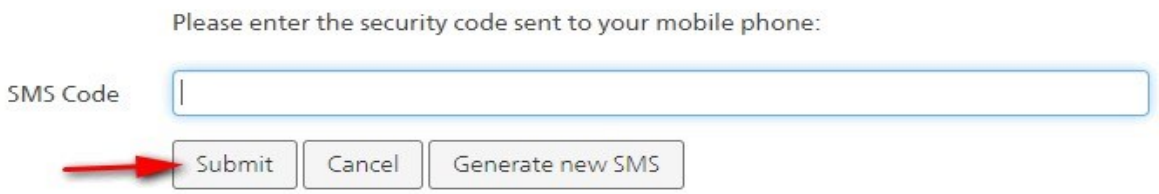
To access MROS goAML Web application entry portal, enter the URL mentioned in the chapter 'Registration':
https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/meldung/registrierung.html

To log in to goAML perform the following steps:

- Enter the Login ID and password and click 'Login with SMS'

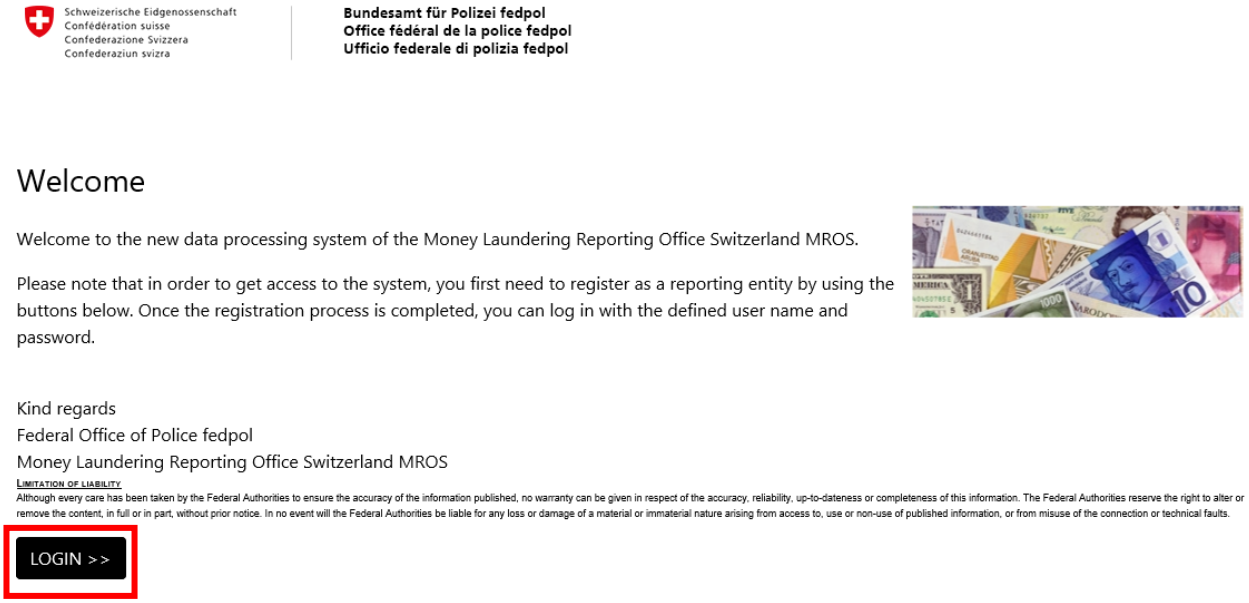


Enter the SMS code sent to the saved phone number and click ‘Submit’.

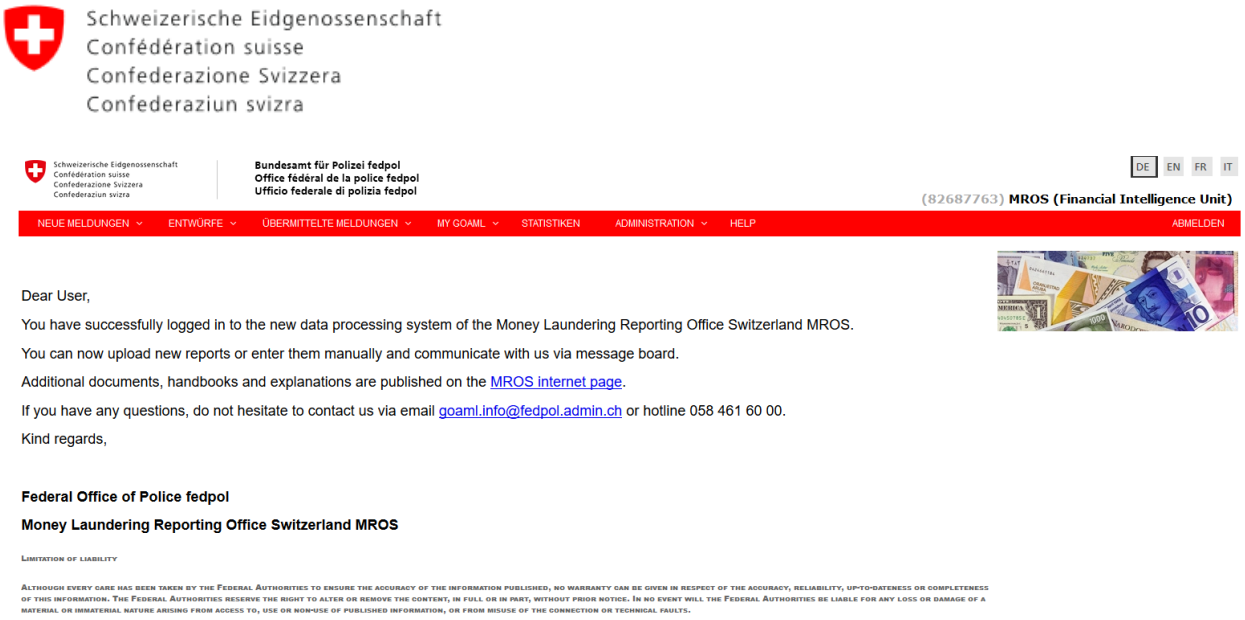


The user is then automatically directed to the goAML welcome page.

- On the welcome page, click the Login button:



- After successfully logging in to the system, the goAML home page is displayed where the desired language in the upper right corner of the screen can be selected:

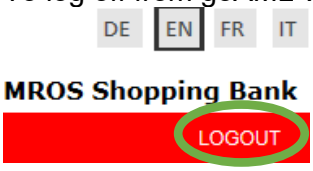


The menu bar of the goAML Web user interface allows the user to navigate to the various goAML Web functions. Hovering with the mouse cursor over a link in the menu bar displays the functions it contains.

Please note: The availability of menu functions depends on your access permissions.

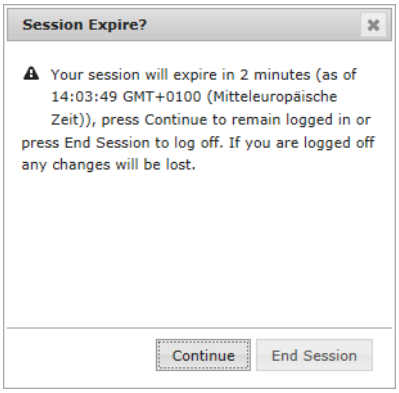
8.2 Logout from goAML

To log off from goAML Web, click Logout (top right) in the menu bar:



- Your goAML session is terminated.

Please note: MROS strongly advises users to frequently save reports being drafted. You will be logged out automatically after a period of inactivity. The following message warns you that all changes will be lost if your session expires.



9 Message Board

The Message Board can be accessed from the main menu bar.

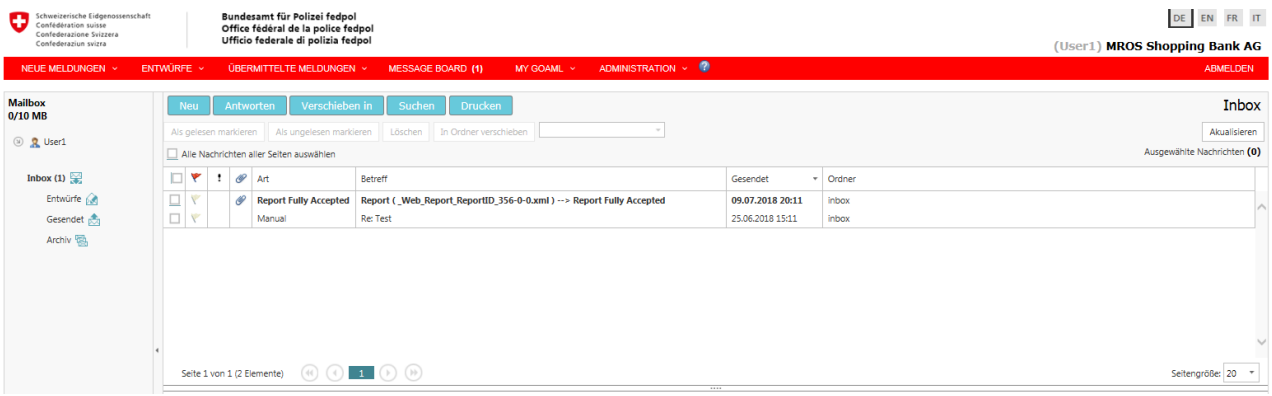
All communication within goAML between MROS and the reporting entities/authorities is conducted through the message board function available in the application. The goAML message board is therefore the internal means of communication between MROS and goAML users. Since the message board **does not correspond to an email functionality**, the various goAML users cannot interact with each other from within goAML. Any communication conducted via message board is only possible with MROS.

The advantage of an internal communication channel is that the communicating parties can interact from within the system. Reporting entities and authorities are notified immediately and automatically if their reports, requests or spontaneous information disclosures are accepted, rejected, being processed or submitted. All information exchanged via the message board is securely stored in the DMZ (see chapter 'goAML IT Architecture').

Notification emails informing that there is an unread item on the message board or notifications related to entity change requests will be sent to the email address registered for the **Organisation** (reporting entity). Individual users are not notified on the email address registered for the user. This is because the message board is a central message repository where all users of the same reporting entity see the same messages, if they are allowed to access the message board. Please note that all notification emails will come from the email address goamlVALIDATION@fedpol.admin.ch (**do not reply to this address as it is not maintained by MROS!**).

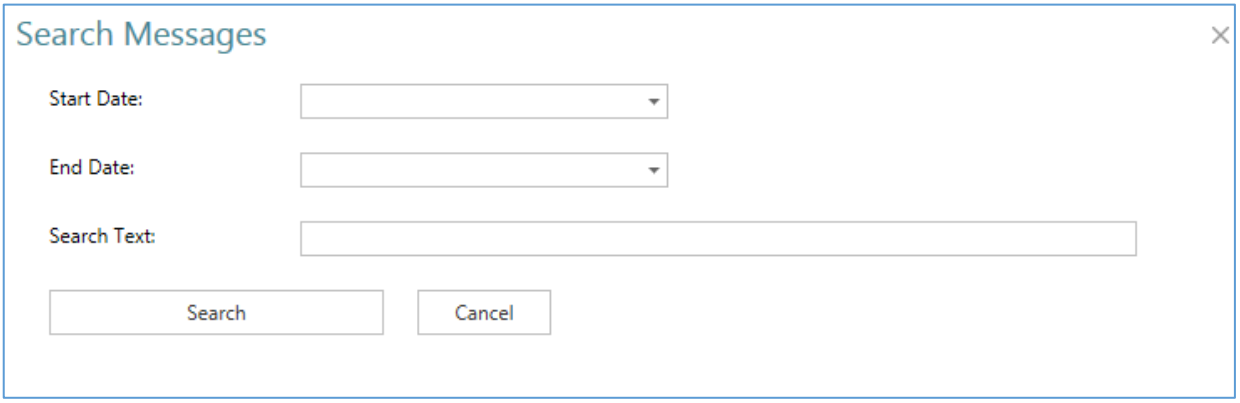
Please note:

- The size to store emails and attachments in the message board is limited to a maximum established by MROS.
- Messages within the message board are automatically deleted by the system 30 days after they have been received or sent.
- Reporting entities may therefore want to ensure that they make copies of all messages and attachments and save them on their internal systems for record keeping purposes.
- For practical reasons, the message board is organized like an email client, although it does not comprise an email functionality.
- **All users of the same reporting entity or stakeholder see the same messages. There are no individual message boxes.**



Message that has been written, sent, or archived can be searched using the Search feature, if they have not

previously been deleted by the automatic deletion mechanism:



Enter the text you want to search for in the Search Text field and click Search. If you want to see only messages within a certain date range, enter the values in the Start Date and End Date boxes.

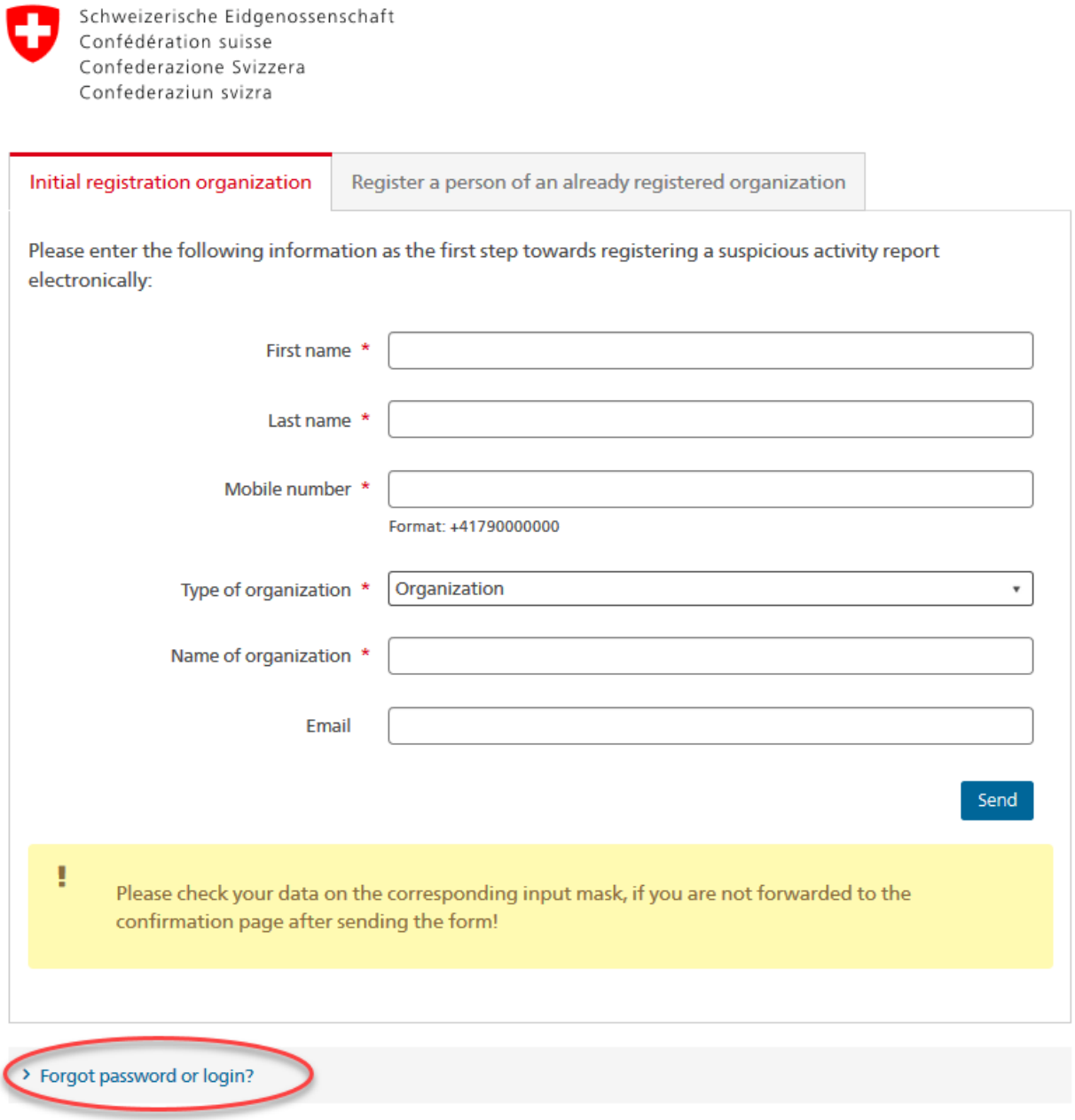
10 My goAML

The 'My goAML' section, which is accessible from the main menu bar, is the personal maintenance section for the individual goAML Web users. Here they can change their password and modify personal/reporting entity data.

Important notice: Each reporting entity is responsible for the management of its user base. This includes adding new users to goAML Web and removing users that no longer require access to it.

10.1 Forgotten password instructions

If you have forgotten your password, please email us stating your LoginID at goaml.info@fedpol.admin.ch by clicking on Reset password request.

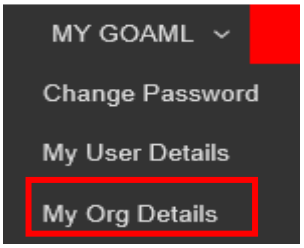


We will then send you a temporary password which you can use to log in. You will automatically be asked by the system to replace this temporary password with a new strong password.

10.2 Change My User/My Organisation Details

When something in the user or reporting entity data changes (e.g. they have a new phone number or change the office address), the goAML Web user/ organisation details must be updated accordingly.

- In the main menu bar select My goAML:



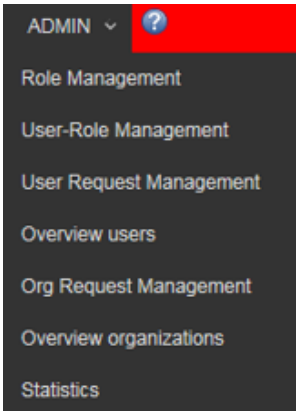
- Select My User Details/My Org Details.
- Make any amendments/additions as necessary.

- Select 'Submit Request'. The changes must first be approved and are then stored in the goAML Web database.

  Note: goAML administrators of the reporting entities can edit only the users of their own reporting entity**. They are obliged to approve new goAML access requests submitted by new users of their reporting entity and to cancel existing access rights, which are no longer needed. This is done by the administrator selecting the Finalize button from the possible selection options** that appear in the request approval screen.

11 Administration

For goAML Web **users with administration rights**, an additional admin menu is available in the menu bar:



With these functionalities the user obtains access to the role and user management features.

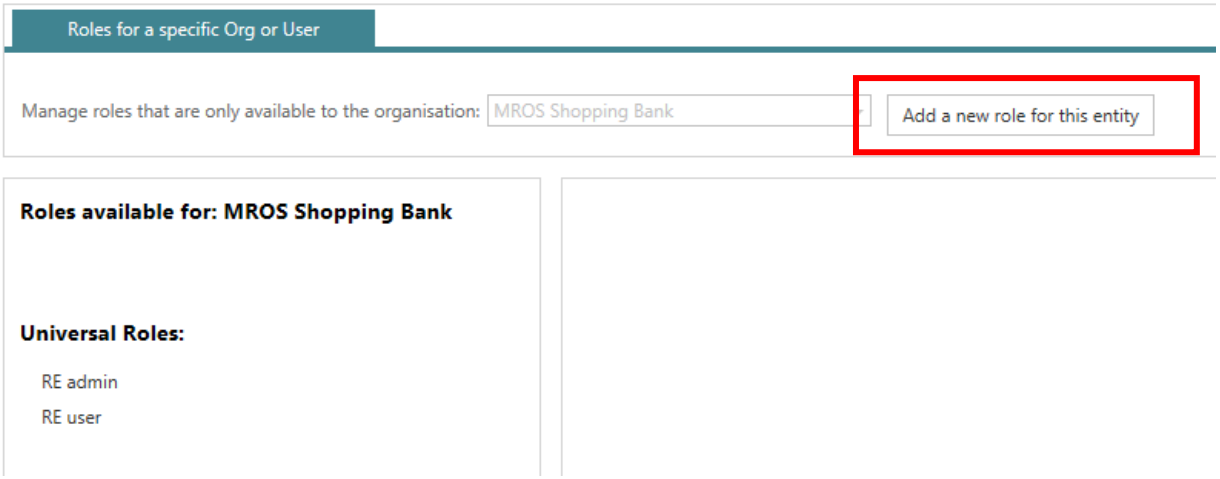
Note: If users see the menu, but not all entries mentioned above, they do not have permission for all of them.

11.1 Role Management

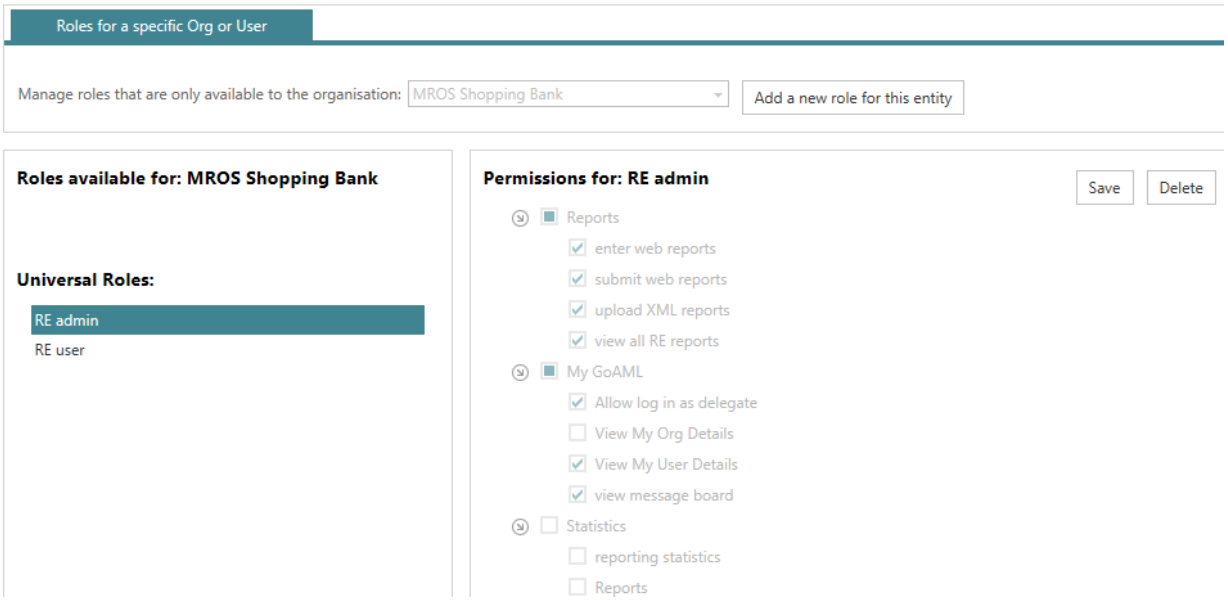
Roles in goAML are permission groups. To fulfil certain tasks, users need a certain set of access permissions. For instance, a controller needs broad access, but not to the maintenance modules, as this is intended for administrators only.

Permission groups (for controllers, administrators etc.) are set up in the Role Management area. Every role defines specific permissions for goAML Web. These roles are assigned to user accounts and thus define the user's permissions.

To create a new role, select the reporting entity from the Roles for Specific Org or User tab and select 'Add a new role for this entity':



After the role has been created, it can be selected in the Roles Available list and the permissions associated with the role can be checked/unchecked, if the user has permission to perform this action. Select Save.



Note: Two role types are available for every reporting entity:

1. User access role
2. Role for the reporting entity's administrators

The permissions for these roles are part of the goAML Web setup and thus cannot be modified. However, administrators can create their own roles with bespoke access permissions at any time.

- To **edit/delete a role**, select the role by clicking its role name, then add permissions by activating, or remove them by deactivating, the respective checkboxes, respectively click on 'Delete' to remove the role. After a security check, the role is deleted and removed for all users.

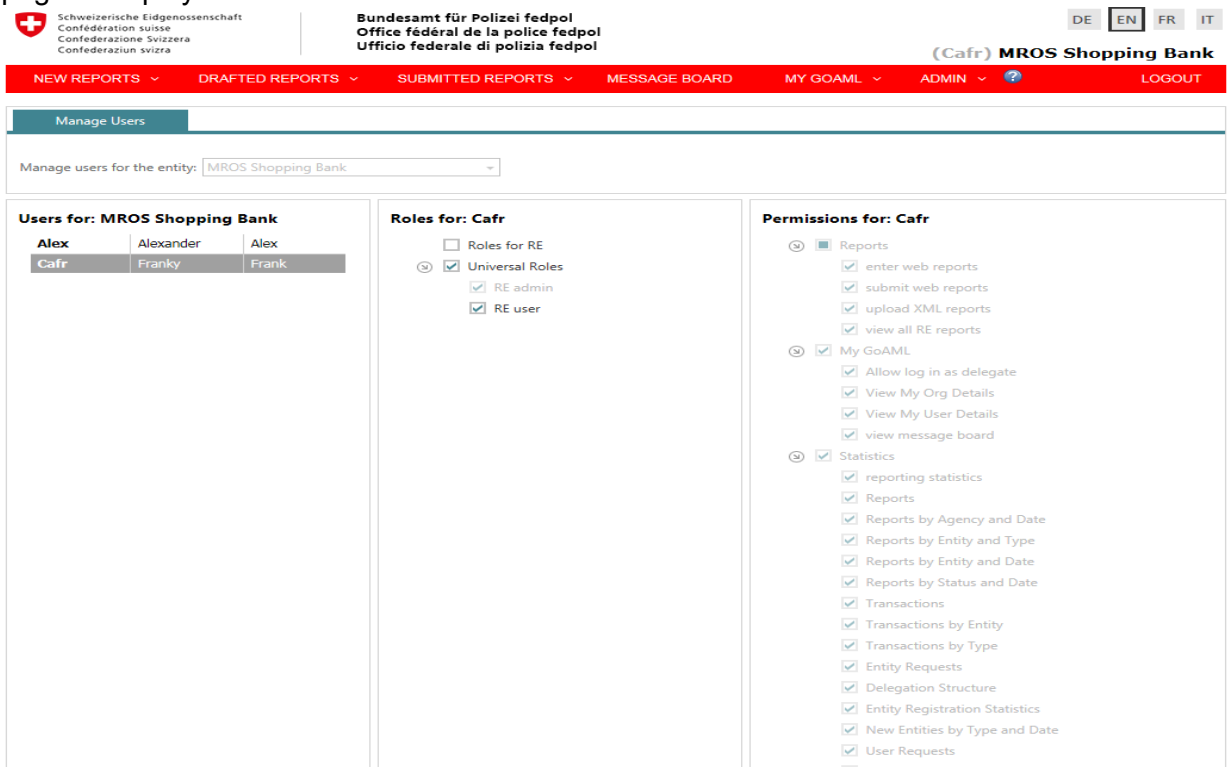
Note: When the deleted role is the last role a user had, the user cannot log in to goAML Web until a new role is assigned to them.

11.2 User Role Management

The User Role Management page allows **administrators** to manage the roles that are mapped to each of the users in an entity.

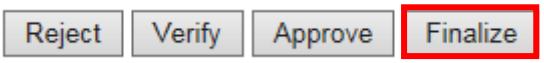
The roles and the permissions associated with the users can be configured as follows:

- Select Admin and then User Role Management from the menu bar. The User Management page is displayed.



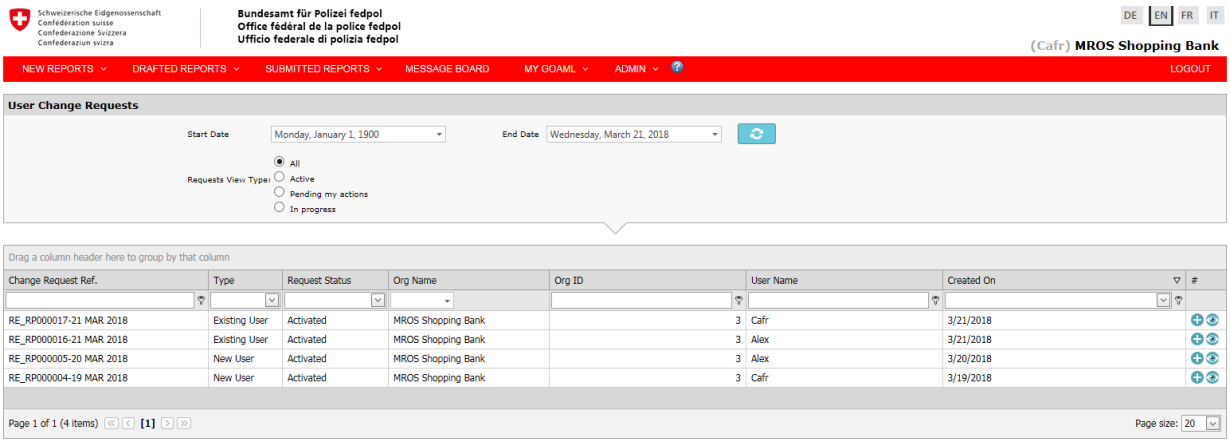
- Selecting the user in the left-hand column shows the associated roles and permissions configured with the selected user.
- Roles and permissions of the selected user can be updated by activating/deactivating some of the checkboxes in the roles and permissions preview columns, if the user has permission to perform this action.
- After making these changes, click Save to save changes. A message appears indicating that the user's roles and permissions have been updated successfully.

Note: goAML administrators of the reporting entities can edit only the users of their own reporting entity. T**hey are obliged to approve new goAML access requests submitted by new users of their reporting entity and to cancel existing access rights, which are not needed any more**. This is done by the administrator selecting the **Finalize** button from the possible selection options that appear in the request approval screen.



11.3 User Request Management

This page allows the administrator to view and manage all the user change requests. The grid is initialised to show the user change requests[3] created in the last month; if another period is to be displayed, enter the Start Date and End Date at the top of the grid and click the refresh button next to it.

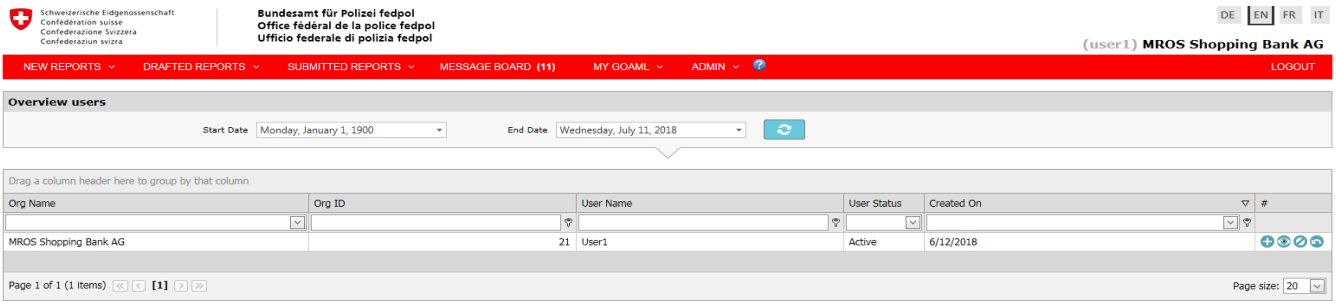


- Click to create a new change request for this user.
- Click to view the details of this user request.

Note: goAML administrators **are obliged to approve new goAML access requests submitted by new users of their reporting entity and to cancel existing access rights, which are no longer needed**. This is done by the administrator selecting the **Finalize** button from the possible selection options that appear in the request approval screen.

11.4 Overview Users

The Overview User management grid allows to view and manage all users registered for a particular reporting entity. When opened, the grid shows the users that were registered during the last month; if another period is to be displayed, enter the Start Date and End Date at the top of the grid and click the refresh button next to it.



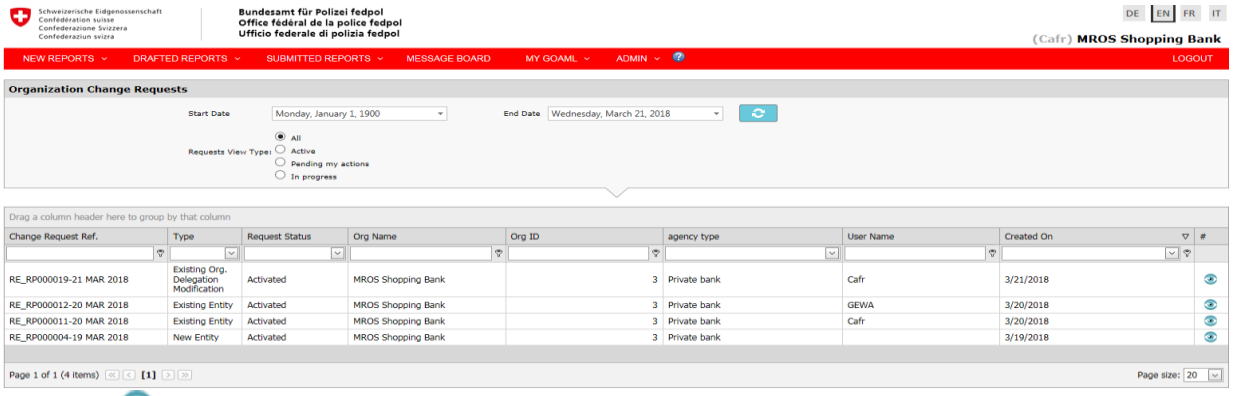
- Click to create a new change request for this user.

[3] Change requests in the context of goAML is referred to any alteration of data or permission concerning a particular user or organisation (e.g. to update the address).

- Click to view the details of this user.
- Click to disable this user.
- Click to reset the password for this user.

11.5 Org Request Management

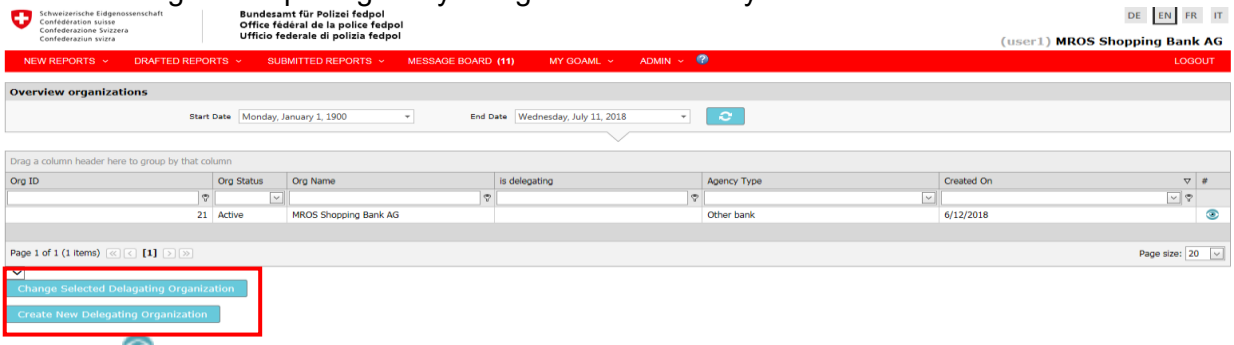
This functionality allows users to view and manage all the organisations change requests. The grid is initialised to show the organisation change requests created in the last month; if another period is to be displayed, enter the Start Date and End Date at the top of the grid and click the refresh button next to it in order to display requested changes within a specified time period.



- Click to view the change requests details.

11.6 Overview organisations

The 'Overview organisations' grid allows the user to view the registration state of its reporting entity and to manage the reporting entity delegation functionality.



- Click to view the details of this reporting entity

At the bottom left corner of the above screen, in the box outlined in red, 2 functionalities related to 'Delegating organisations' are visible. A reporting entity can decide to delegate its reporting function to another reporting entity.

- Click Change Selected Delagating Organization to make a change request **to MROS** for appointing a selected reporting entity to be delegated.
- Click Create New Delegating Organization to register a new delegating reporting entity in goAML.

12 Application Support and System Maintenance

Should the reporting entity encounter an issue with the goAML application, please notify MROS at your earliest convenience. If the system is available: Please use the Message Board for this communication. Otherwise, please contact MROS at goaml.info@fedpol.admin.ch or call +41 58 461 60 00.

System maintenance and updates will be carried out on the goAML application on a regular basis. During these periods, it may be necessary to take the application offline. Correspondence detailing this down time will be provided in advance via goAML homepage.

13 Glossary

The following list explains terms and abbreviations used in conjunction with the goAML Web application:

Term	Explanation
Change request	Any request to alter data or permissions concerning a particular user or organisation (e.g. to update the address).
Supervisory authority	The Swiss supervisory authorities are: the Financial Market Supervisory Authority (FINMA), the Swiss Gaming Board (SGB), the recognised self-regulatory organisations and the Intercantonal Supervisory and Executive Authority under Article 105 GamblA
DMZ	Demilitarized zone (located in Switzerland), being a secure IT environment protecting from unwanted access to the servers located in it.
goAML	Intelligence analysis system developed by United Nations Office on Drugs and Crime intended to be used by the FIU (Financial Intelligence Unit) to combat money laundering
GUI	Graphical User Interface
Reporting Entity (RE)	**R**eporting **E**ntity - Financial intermediary, merchant or authority authorized to submit suspicious activity reports in Switzerland based on the Anti- Money Laundering Act (AMLA) and/or the Swiss Criminal Code
Stakeholder	Any user registered in goAML Web and being authorized to submit suspicious activity reports to MROS based on the Anti-Money Laundering Act (AMLA) and/or the Swiss Criminal Code.
Supervisory Body	This term includes supervisory bodies active in Switzerland, namely the Swiss Financial Market Supervisory Authority (FINMA), the Federal Gaming Board (FGB), the recognised self-regulatory organisations (SRO) and the inter-cantonal supervisory and executing authorities in accordance with Art. 105 GamblA.
Tooltip	Quick info window that is displayed when a user hovers the mouse pointer over a field
UNODC	United Nations Office on Drugs and Crime, which is the developer of goAML

Disclaimer

Limitation of liability

Although every care has been taken by the Federal Authorities to ensure the accuracy of the information published, no warranty can be given in respect of the accuracy, reliability, up-to-dateness or completeness of this information.

The Federal Authorities reserve the right to alter or remove the content, in full or in part, without prior notice.

In no event will the Federal Authorities be liable for any loss or damage of a material or immaterial nature arising from access to, use or non-use of published information, or from misuse of the connection or technical faults.