

Contents

1	Requirements for using the eIAM portal	1
2	Setting up and changing user administrators for companies	1
3	Systems	2
3.1	CH-LOGIN.....	2
3.2	User administration (eIAM portal)	2
3.3	Logging into the eGov portal.....	2
4	Setting up and changing users	3
4.1	Logging into the eIAM portal.....	3
4.2	Setting up a new user	3
4.3	Onboarding status overview	6
4.4	Authorisation roles:.....	7
4.5	Business roles	8
4.6	eSubmission "Medi-restricted" application role	8
4.7	Changing a user	9
4.8	Deactivate, delete/archive user.....	9
5	Add correspondence e-mail address (eSubmission / EIViS)	10
6	Creating user accounts for employees of other companies	10
7	Security notice	11
8	Contact	11

Change history

Version	Valid and binding as of	Description, comments	Author's initials
2.0	16.11.2020	Addition to section on logging into eGov portal and authorisation roles for other eGov services	xrr, anm
1.0	06.09.2019	New document due to eIAM migration VM-ID: OS000_00_008d_MB to replace ZL000_00_031d_MB	hoa, anm

1 Requirements for using the eIAM portal

To use the eIAM portal as a user administrator, it is necessary to sign up to the Swissmedic website (www.swissmedic.ch/egov-portal-registration).

2 Setting up and changing user administrators for companies

Once a user license agreement with Swissmedic has been signed, Swissmedic sends an invitation email to the user administrators stated in the contract. These users can register themselves on the eIAM portal and set up new user accounts for their company. After the user administrator account is set up, the administrator receives an e-mail from eiamnoreply-prod@bit.admin.ch with an onboarding code plus an e-mail from it@swissmedic.ch with registration information..

Any changes to the details of the user administrators can be reported to the Swissmedic IT Service Centre (ISCS) by phone or in writing.

3 Systems

3.1 CH-LOGIN

A CH-LOGIN (Federal Administration account) is required in order to access the eGov portal. Each user (including user administrators) must create a CH-LOGIN account to access the eGOV portal. A telephone number and some security questions must be entered for the two-factor authentication process and to reset the personal password.

Note: Each user can change the login details (phone number, email, password) of their own CH-LOGIN account.

For more information about the CH-LOGIN account, visit:

<https://www.bit.admin.ch/bit/de/home/dokumentation/ch-login.html>

3.2 User administration (eIAM portal)

The eIAM (eGovernment Identity and Access Management) portal is used for "delegated administration" (<https://www.portal.eiam.admin.ch/portal/adminservice/app/home>).

3.3 Logging into the eGov portal

To access the eGov applications which your company is authorised to use, please follow this instruction.

Requirements:

PC: Internet Explorer/Microsoft Edge and Mozilla Firefox are tried and tested browsers

Mac: Mozilla Firefox (the "Safari" browser is not suitable)

1. Call up the URL www.swissmedic.ch in your browser's address bar
2. Click the "eGov Portal (applications)" link in the top right corner,

or, alternatively, type portal.swissmedic.ch into your browser's address bar and press "ENTER/OK" on your keyboard.

Menu page for the various eGov services:



1. **Reporting portals:** CPP, eMessage, eSubmission, GMP-GDP, Licences, OCABR, Safety communication
2. **MyAccount:** CH-LOGIN Personal Federal Administration account (*here anyone can adjust their access data, such mobile no. or password, themselves*)
3. **Partner Administration:** User management for use within your own company (for user administrators only)
4. **EIViS:** (Electronic Vigilance Reporting Portal)
5. **MESA:** (Narcotics)

4 Setting up and changing users

4.1 Logging into the eIAM portal

User administrators log into <https://www.portal.eiam.admin.ch> with their CH-LOGIN account



Selection of login procedures

Please select with which login procedure you would like to access the application of your
You can find out more about the individual procedures in the help.

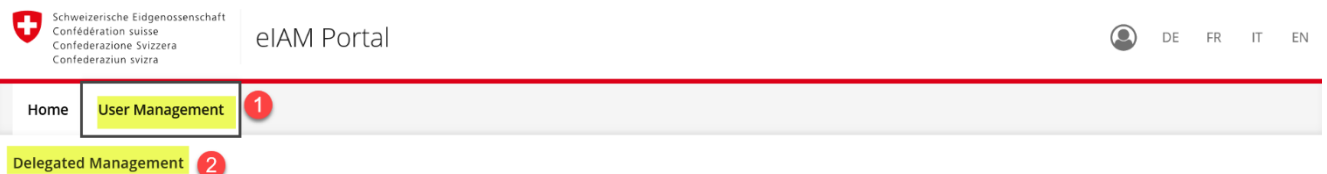


4.2 Setting up a new user

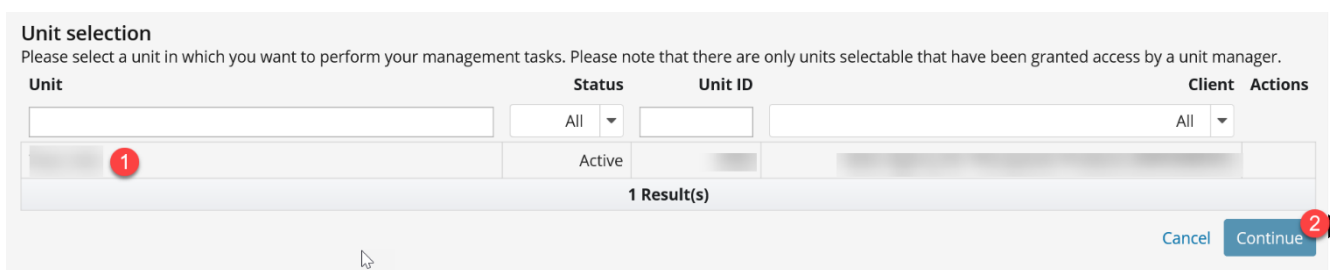
Note:

The user administrator can also authorise the employees of a third-party company.

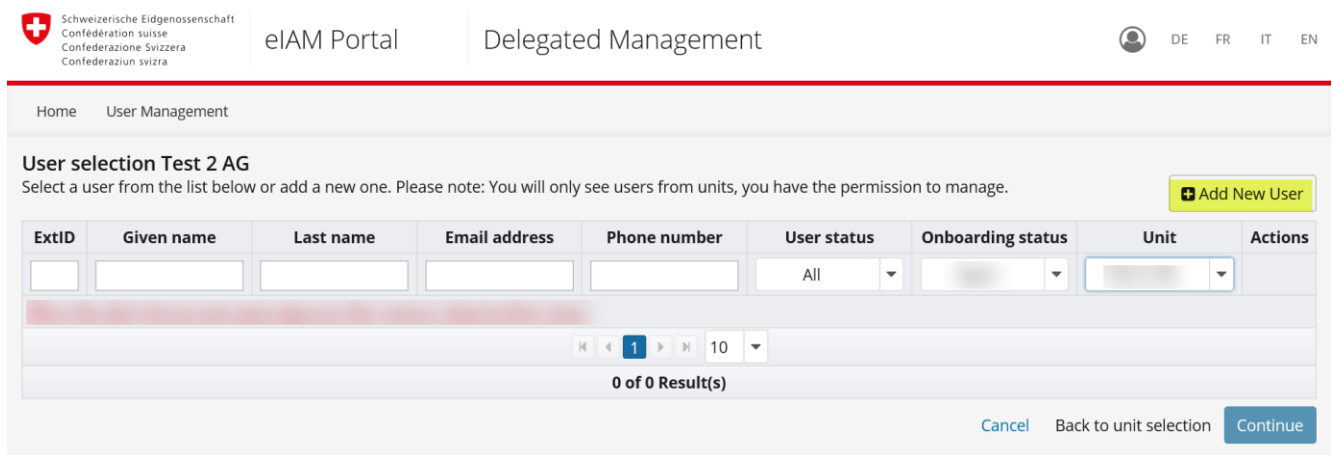
To create a new user, select (1) *User Management* and (2) "*Delegated Management*".



Select the unit (company) from the *Unit selection* menu and then confirm your selection by pressing "**Continue**".



Click the “Add New User” button.

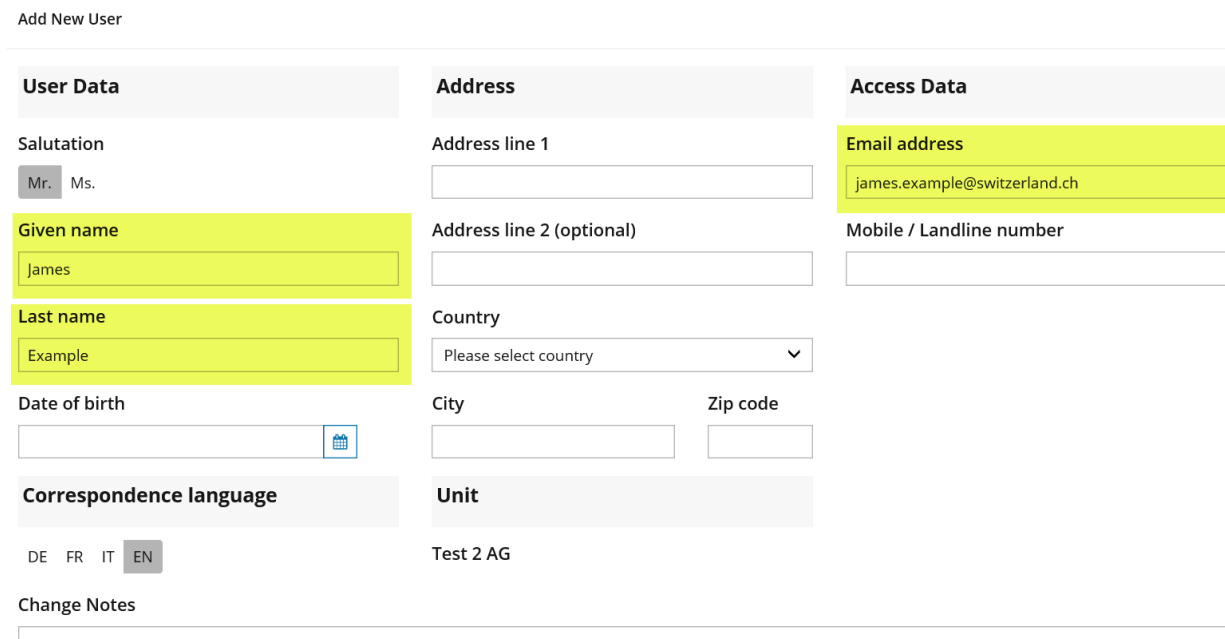


The screenshot shows the 'eIAM Portal' interface under 'Delegated Management'. It features a navigation bar with 'Home' and 'User Management'. The main content area is titled 'User selection Test 2 AG' and includes a note: 'Select a user from the list below or add a new one. Please note: You will only see users from units, you have the permission to manage.' A yellow 'Add New User' button is visible in the top right. Below is a table with columns: ExtID, Given name, Last name, Email address, Phone number, User status, Onboarding status, Unit, and Actions. The table is currently empty, showing '0 of 0 Result(s)'. At the bottom right, there are 'Cancel', 'Back to unit selection', and 'Continue' buttons.

Enter the user details in the window that appears now.
The **Given name** and **Last name** and **Email address** are mandatory. The other fields are optional and not relevant for access to the eGov portal.

Note:

The "Mobile / Landline number" field required for the two-factor authentication (mTAN) is stored with the user's CH-LOGIN account.



The 'Add New User' form is divided into three main sections: 'User Data', 'Address', and 'Access Data'.
User Data: Includes 'Salutation' (Mr./Ms.), 'Given name' (James), 'Last name' (Example), 'Date of birth' (with a calendar icon), and 'Correspondence language' (DE, FR, IT, EN).
Address: Includes 'Address line 1', 'Address line 2 (optional)', 'Country' (Please select country), 'City', and 'Zip code'.
Access Data: Includes 'Email address' (james.example@switzerland.ch), 'Mobile / Landline number', and 'Unit' (Test 2 AG).
 The 'Given name', 'Last name', and 'Email address' fields are highlighted in yellow to indicate they are mandatory.

Once you have entered the user details, press “Save and continue”. You will now be taken to the "Manage permissions" page.

User administrators can assign the following roles/permissions to the users. Only the roles that correspond to the scope of use are available for selection.

Home User Management

Swissmedic eIAM Portal Delegated Management

Manage permissions

Unit	Given Name	Last name	Email address	Phone number	User ID
Test 2 AG	James	Example	james.example@switzerland.ch		464627

Profile-CHL1020100185
465265

Applications

- ELVIS - Electronic Vigilance System
- Swissmedic - eSubmissions Platform

Business roles

- ELVIS_DIRECT-INSERT
- ELVIS_FILE-UPLOAD
- MLP_ESUBMISSIONS-MEDI-FULL
- MLP_ESUBMISSIONS-MEDI-RESTRICTED

Roles

- mlp-appl-download
- mlp-appl-read
- mlp-appl-submit
- mlp-appl-upload
- mlp-cpp

Application	Role
Swissmedic - eSubmissions Platform	appl-download
Swissmedic - eSubmissions Platform	appl-submit
Swissmedic - eSubmissions Platform	appl-read
Swissmedic - eSubmissions Platform	appl-upload
Swissmedic - eSubmissions Platform	private

Granted Permissions

Granted	Application	Role	Attribute	Action
---------	-------------	------	-----------	--------

Back to User Selection Continue

Once you have selected the application roles and/or business roles (see [Authorisation roles](#)) press the “Continue” button. This takes you to an overview of the user you have just entered. You can complete the process by pressing the “Send onboarding email” button:

Home User Management

Overview

Unit	Given Name	Last name	Email address	Phone number	User ID
Test 2 AG	James	Example	james.example@switzerland.ch		464627

Granted Permissions [Show more](#)

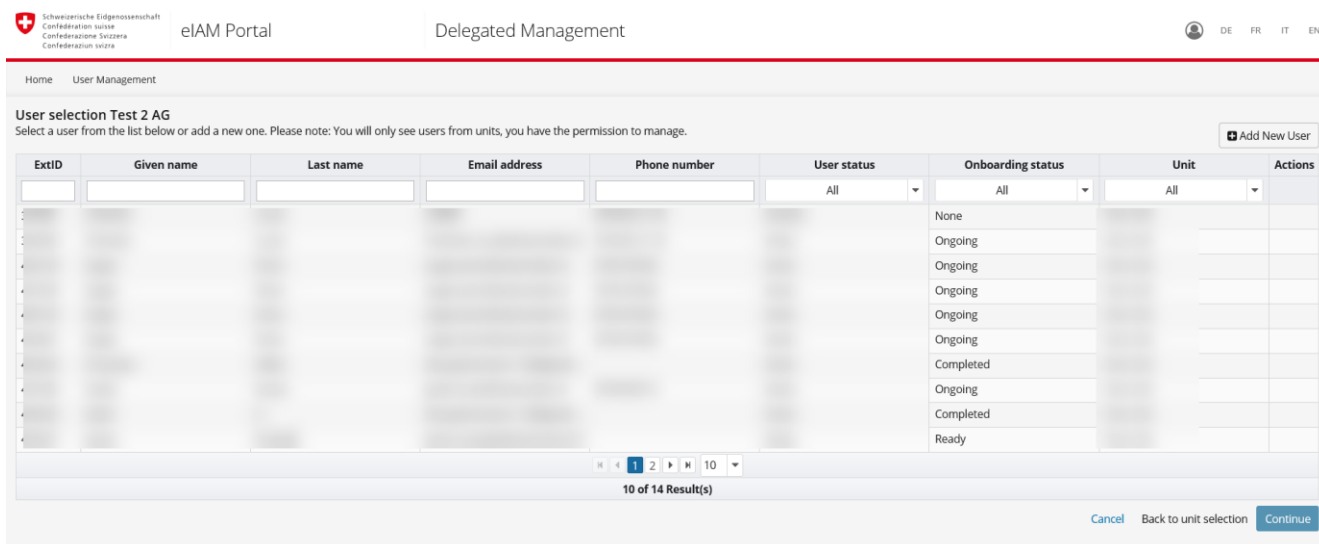
Justification for Permission (traceability)

Back to Grant Permissions [Send onboarding email](#) [Start onboarding manually](#)

The user will then receive an onboarding email with an onboarding link to complete their registration.

4.3 Onboarding status overview

Use the Delegated Management option under User Selection to check if the users you authorised have followed the link to the CH-LOGIN account.



The screenshot shows the 'Delegated Management' interface in the eIAM Portal. It features a table for user selection with the following columns: ExtID, Given name, Last name, Email address, Phone number, User status, Onboarding status, and Unit. The 'Onboarding status' dropdown menu is open, displaying options: None, Ongoing, Ongoing, Ongoing, Ongoing, Ongoing, Completed, Ongoing, Completed, and Ready. The table shows 10 of 14 results. Navigation buttons include 'Cancel', 'Back to unit selection', and 'Continue'.

Onboarding Status	Description
In process / ready	User has been entered, onboarding email is being sent.
Ongoing	The user has not yet used the onboarding code.
Overdue	The onboarding code is still valid but will expire soon. > Notify user
Expired	The onboarding code has expired (is only valid for a limited amount of time) > user administrator must send a new onboarding code. You can send a new onboarding link to the user by selecting the user's name under the company and then selecting Action.
Completed	Onboarding process completed, user has been successfully linked to their CH-LOGIN account.

4.4 Authorisation roles:

Allocating individual application roles:

User administrators can only see the application roles that have been approved for their company.

eSubmissions:

Role	Description
appl-read	If this role is assigned, the user has read access to the whole dashboard (see also the roles " <i>medi-full</i> " and " <i>medi-restricted</i> ").
appl-upload	If this role is assigned, the user additionally has the right to upload or modify documents relating to an application.
appl-download	If this role is assigned, the user additionally has the right to download and view documents.
appl-submit	If this role is assigned, the user additionally has the right to submit an application.
private	Required role for access to application
medi-full	If this role is assigned, the user has access to all the company's preparations.
medi-restricted	If this role is assigned, the user only has access to the explicitly specified preparations.

EIViS:

Role	Description
direct-insert	Authorisation for EIViS (direct-insert)
file-upload	Authorisation for EIViS (file-upload)
hcp-direct-insert	Authorisation for EIViS (direct-insert) – specifically for hospital pharmacies
hcp-file-upload	Authorisation for EIViS (file-upload) – specifically for hospital pharmacies
mah	The user is recognised as a company user.
private	Required role for access to application

MESA:

Role	Description
evaluator	This authorisation is only available to cantonal pharmacists and cannot be inherited
sender	This authorisation allows the user to write MESA reports
private	Required role for access to application

Other eGov services:

Role	Description
CPP	If this role is assigned, the user can submit CPP orders via the eSubmission platform.
eMessage	If this role is assigned, the user can submit medical product documentation via the eSubmission platform.
gmp-gdp	If this role is assigned, the user can submit GMP/GDP certificate orders via the eSubmission platform. Here it is important also to assign the role "mlp-appl-read"
licences	Once this role has been assigned, significant changes to equipment, installations and procedures can be reported to Swissmedic

Role	Description
ocabr	With this role, the user can submit documentation on OCABR services.
safety-com	With this role, the user can submit documentation on signals.

Note: The “mlp-private” role is required for all applications.

4.5 Business roles

The business role is a package of application roles. This makes it easier to assign authorisations as only one business role needs to be assigned. The following business roles are currently available:

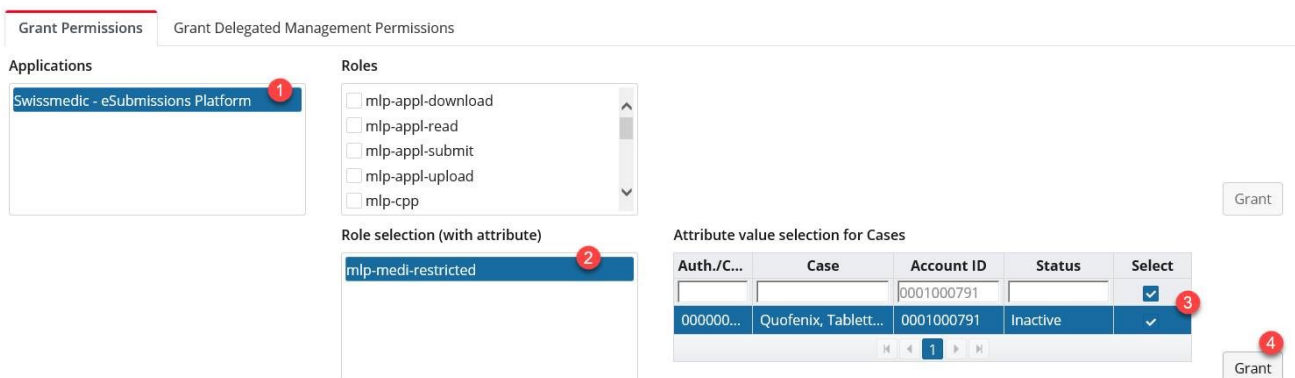
Business role	Description	Roles of business role
ELVIS_DIRECT-INSERT	Includes all the roles required to capture an adverse reaction report in EIViS.	direct-insert, mah and private
ELVIS_FILE-UPLOAD	Includes all the roles required to upload an XML file for an adverse reaction report.	file-upload, mah and private
MESA_SENDER	Includes all the roles required to transmit reports in MESA and to conduct evaluations	sender and private
MESA_EVALUATOR	Includes all the roles required in order to look up reports	evaluator and private
MLP_ESUBMISSIONS-MEDI-FULL	Includes all the roles required in order to submit a delivery to the eSubmission platform for approval.	appl-download; appl-submit; apple-read, appl-upload, medi-full and private

4.6 eSubmission "Medi-restricted" application role

The "Medi-restricted" role is used if only specific preparations are to be allocated to a user. In this case, the “medi-full” role must not be allocated.

You can allocate the authorisations for the “medi-restricted” role as follows:

1. Under Applications > eSubmission platform
2. In the Role selection field, click “mlp-medi-restricted”.
3. Select the preparations you wish to allocate to the user (multiple selections are possible)
4. Next press the “Authorise” button and start the onboarding process as in the “Create new user” section.



The screenshot shows the 'Grant Permissions' interface. It is divided into two tabs: 'Grant Permissions' (active) and 'Grant Delegated Management Permissions'. Under 'Grant Permissions', there are three main sections:

- Applications:** A list containing 'Swissmedic - eSubmissions Platform' (marked with a red '1').
- Roles:** A list of roles with checkboxes: mlp-appl-download, mlp-appl-read, mlp-appl-submit, mlp-appl-upload, and mlp-cpp.
- Role selection (with attribute):** A list containing 'mlp-medi-restricted' (marked with a red '2').

Below the role selection is a table for 'Attribute value selection for Cases':

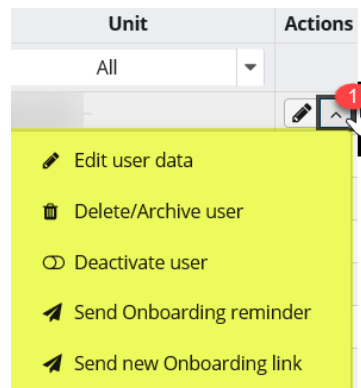
Auth./C...	Case	Account ID	Status	Select
		0001000791		<input type="checkbox"/>
000000...	Quofenix, Tablett...	0001000791	Inactive	<input checked="" type="checkbox"/> (marked with a red '3')

At the bottom right of the interface, there is a 'Grant' button (marked with a red '4').

4.7 Changing a user

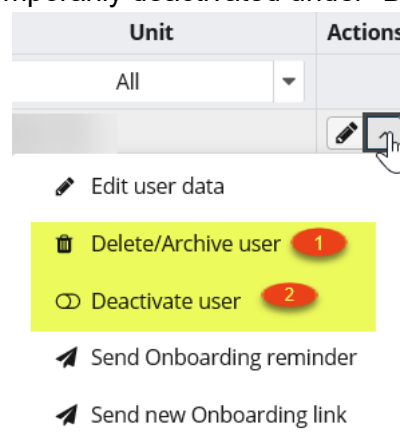
The user administrator can change a user with the following actions:

- Delete/archive user (e.g. departure from the company)
 - Deactivate user (if the user is to be temporarily denied access to the portal)
 - Activate user (if the user was previously deactivated)
 - Give the user access to certain preparations (medi-restricted role)
- Click the icon below the no. 1 (Actions column).



4.8 Deactivate, delete/archive user

1. Under “Delete/Archive user”, the user can be marked for deletion/archiving (e.g. departure from company). The user account is then barred from accessing Swissmedic applications. The final deletion/archiving takes place three months later.
2. The user account can be temporarily deactivated under “Deactivate user”.

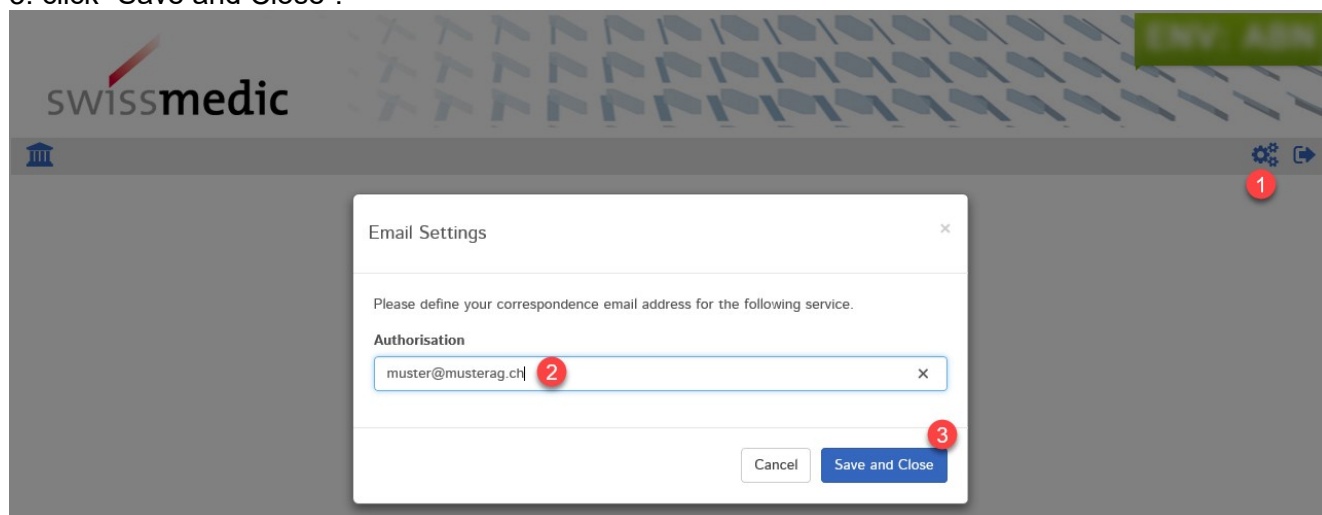


Both options allow the user to be reactivated, except that the “Delete/Archive user” option only allows this within the first three months.

5 Add correspondence e-mail address (eSubmission / EIViS)

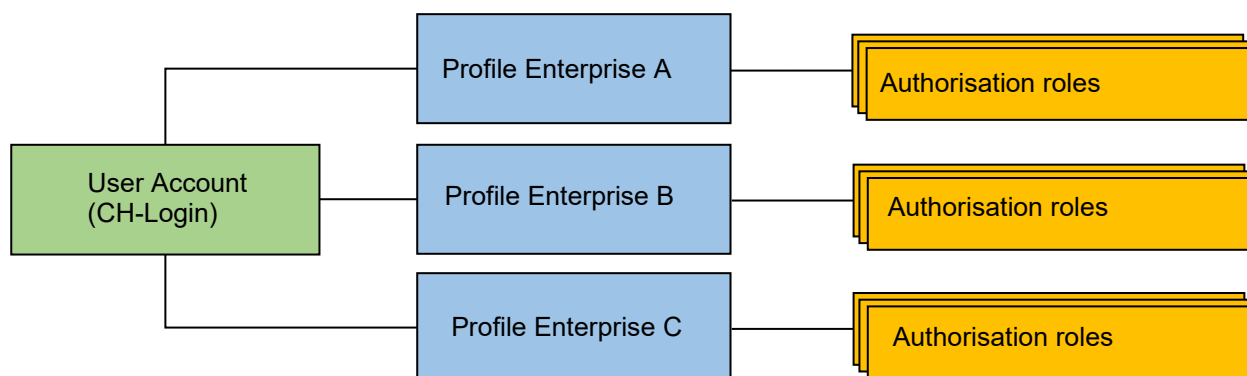
The user administrator can add a correspondence e-mail address into eSubmission / EIViS depending on the authorization. Log into the eIAM portal and select the appropriate application: Swissmedic - eSubmission Platform or EIViS - Electronic Vigilance System. This function is not available for all other services.

1. click on "Settings" (gear symbol)
2. add the main correspondence e-mail address
3. click "Save and Close".



6 Creating user accounts for employees of other companies

A natural person with a CH-LOGIN account can now also manage the users of multiple companies. The person must select a profile when logging in. The profile represents the company for which the user is authorised. This function is only possible if **the same email address** is used for all the user accounts. Otherwise, it is not possible to link multiple profiles (companies) to one user account.



7 Security notice

User administrators are responsible for ensuring that only authorised persons are given access to the Swissmedic eGov Services (specialist applications) via the eIAM portal. Users who do not log in for more than half a year are deactivated. User administrators can reactivate these users. Any user administrator who has been deactivated should contact the Swissmedic IT Service Centre (ISCS).

8 Contact

If you have any problems with the **CH-LOGIN account** (Federal Administration eIAM portal) please contact:

BIT (Swiss Federal Office of Information Technology, Systems and Telecommunication) Service Desk

Phone: +41 58 465 88 88
servicedesk@bit.admin.ch

For any other **administrative queries** please contact:

Swissmedic IT Service Centre (ISCS)

Phone: +41 58 462 06 00 (07h30 – 17h30)
it@swissmedic.ch