Národní organizace
pro ověřování
pravosti léčiv

Czech Alert Management System (CZAMS)
Web portal

End user guide (pharmacies, wholesalers)

Release 9.0

14th November 2026

Národní organizace pro ověřování pravosti léčiv

CONTENTS

CZAMS – End Users | User Guide | Release 9.0

PART I BASIC INFORMATION & ACCESS 3

1 Introduction 4
2 Alert Management System 5
3 Notifications, Deadlines & Escalations 6
4 Archiving 7
5 IT Security 8
6 Access Credentials 9
7 Logging In 10
8 Two-Factor Authentication 11
9 Main Menu 14
10 Changes, News & Notifications 15
11 Dashboard 16

PART II USER MANAGEMENT 21

12 User Management — Dashboard 22
12.1 User List 23
12.2 Adding a User 24
12.3 Editing a User 26

PART II USER MANAGEMENT (continued)

12.4 My Profile 30
12.5 API Keys 32
12.6 Multi-factor Authentication 33
12.7 Notifications 34
12.8 Audit 36

PART III ALERT MANAGEMENT 37

13 Alert Management 38
13.1 Controls 39
13.2 Configuring List Columns 41
13.3 Export 42
13.4 Summary Export 43
13.5 Filters 44
13.6 Bulk Status Change 46
13.7 Alert Details 48
13.8 Alert Groups 50
14 Communication with MAH/OBP 53
14.1 Communication with CZMVO 54

PART III ALERT MANAGEMENT (continued)

14.2 Requests for Additional Information 57
15 Alert Details — Processing 58
15.1 Alert Status Change 60
15.2 Time to Change a Closed Alert 61
16 Exceptions 62
16.1 Verifying an Exception 63

PART IV SUPPLEMENTARY INFORMATION 64

17 End User Procedural Errors 65
17.1 Printing the Resolution Report 69
17.2 Procedural Errors — Overview 70
18 Changes in CZAMS 71

PART V ALERT STATUSES & RESOLUTION 73

19 Alert Resolution — Terms 74
20 CZMVO Pre-analysis 75
21 Initial Alert Statuses 80
22 Escalation Statuses 81
23 Intermediate Alert Statuses 82
24 Final Alert Statuses 83

PART I

Basic Information and System Access

INTRODUCTION

Purpose of the document

This guide is intended for MAHs/OBPs, but it may also provide information to other users of the Alert Management System who manage their alerts via the CZAMS web interface.

The examples given in this guide are therefore aimed mainly at MAHs/OBPs. The set of functions available to MAHs/OBPs differs from the functions available to wholesalers and pharmacies.

Prerequisites for using the system

- ✓ The MAH/OBP has received the primary administrator access credentials for the Czech Alert Management System. NOOL sends these on request. (This is required even if the MAH/OBP communicates with CZAMS via the API.)

Note: **The administrator then manages other users and their permissions (**including the sending of notifications**) independently.**

Terminology*

Czech Medicines Verification Organization – CZMVO (Národní organizace pro ověřování pravosti léčiv, z.s., – NOOL)

A non-profit organisation that ensures the implementation and operation of the National Medicines Verification System (NSOL) in the Czech Republic.

CZAMS – CZMVO Alert Management System

A system complementary to the National Medicines Verification System (CZMVS), operated by CZMVO, which is used for managing and investigating alerts raised in the CZMVS.

Alert Level 5

At this incident level, a system notification is always generated; the party at which the alert was raised (i.e. the end user, the MAH/OBP, the parallel distributor) is informed of it, as are CZMVO and SÚKL (State Institute for Drug Control).

*Further definitions of terms can be found in Part IV, “Alert Statuses and Their Resolution”

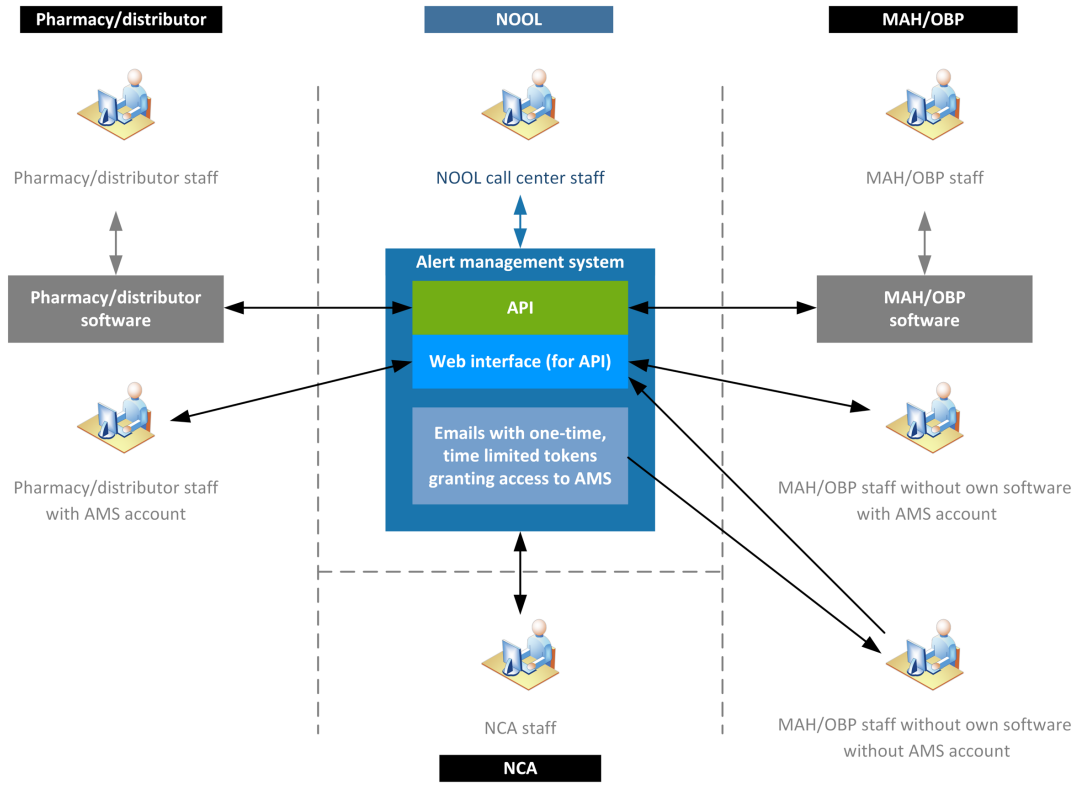
CZMVO ALERT MANAGEMENT SYSTEM

The CZMVO Alert Management System (CZAMS), developed and operated by CZMVO/NOOL, is a support system to the Czech Medicines Verification System (CZMVS). Its purpose is to ease the administration associated with alert investigation and thereby help simplify and speed up the entire investigation process.

Alerts raised in the Czech Republic can be managed in three ways:

- ✓ Through **full access** to the **web interface** of the NOOL Alert Management System (CZAMS). **This option is the main subject of this guide.**
- ✓ Through **one-time, time-limited** access in the CZAMS web interface to a specific alert only. The access link, including a token, is sent in an automatically generated e-mail. See the User Guide for One-time Limited Access to CZAMS https://www.czmvo.cz/file.php?id=873
- ✓ By integrating the user's own alert management system with the NOOL Alert Management System using **API communication.**

  Note: A technical description of the **API interface** can be found in the document "Technical documentation for developers – description of API. https://www.czmvo.cz/en/alert-management/producers-mah-parallel-distributors/



NOTIFICATIONS, PROCESSING DEADLINES, ESCALATIONS

System notifications

System notifications are sent to those users who have them activated in their settings under **User Management.** Individual notification types can be switched off or on according to the user's needs; however, there must always be at least one recipient of each type of system notification within the organisation.

Notifications of new alerts

END-USER TRANSACTIONS

a) Technical error by the end user (A2, A3, A68, A52) – the MAH/OBP receives information about the new alert from CZAMS **immediately**.

b) Procedural error by the end user (A7, A24) – the MAH/OBP receives information about the new alert from CZAMS **48 hours** after the alert was raised.

MAH/OBP TRANSACTIONS

MAHs/OBPs also receive information about alerts raised during an MAH/OBP transaction or a parallel distributor's transaction**, always in bulk for all alerts from the previous day.**

If the **MAH requests additional information** about an alert from the end user and the end user does not respond, the end user receives a reminder **48 hours** after the request was made, and another one 5 days after the request was made. **If there is still no response, SÚKL may be informed of the end user's inactivity.**

Investigation period

An alert should be investigated and **closed** as soon as possible, within **14 days of being raised**, which is the statutory period during which a medicinal product may be held in a pharmacy. After this period, the product should be returned from the pharmacy to the wholesaler.

The 14-day period is defined by Act No. 44/2019 Coll., Section 89, subsection 4.

Inactivity notifications (escalations)

END-USER TRANSACTIONS

a) Technical error by the end user (A2, A3, A68, A52) - If the parties involved are inactive, both the MAH/OBP and the end user receive the first notification after **5 days** and the second after **10 days** from the alert being raised.

b) Procedural error by the end user (A7, A24) - The MAH/OBP receives the information after **48 hours** and can start resolving the alert immediately. Until then, the deadline for resolution lies with the end user. Only the end user is notified of inactivity; the MAH/OBP does not receive inactivity notifications.

MAH/OBP TRANSACTIONS

If the MAH/OBP is inactive, it receives the first escalation after **5 days** and another one after **10 days** from the alert being raised.

ARCHIVING

Archiving

After 90 days, a closed alert is marked with the "Archive" flag. After this time, the alert status can no longer be changed, but the alert is still visible in the system.

Note: Within the 90 days, an alert marked with the "Archive" flag can be **restored** and the investigation continued. However, this applies only to alerts that were **closed with a status that does not allow the pack of the medicinal product to be dispensed**. If the medicinal product has already been dispensed, i.e. it is no longer available, the investigation cannot be reopened.

After 5 years, the **closed alert** is moved to the **archive** and is no longer visible in the Alert Management System. **After 7 years**, all alert data are **deleted**.

IT SECURITY

Two-factor authentication for the web interface

Two-factor authentication has been implemented for access to the web interface. **E-mail** and/or **Google Authenticator** can primarily be used as the second factor.

The type of second factor can be set by the administrator, or by the user themselves in the user management of the given organisation.

Time limit for web login

Automatic logout of the user after a defined period of inactivity (currently **4 hours**) has been implemented.

Account lockout after several failed logins

If a user repeatedly enters an incorrect password when accessing the web interface, the account is locked for a defined period. (Currently **3 failed attempts = 60 minutes of lockout**.)

Login page attribute setting

Automatic pre-filling of credentials on the login page is disabled to prevent certain types of attacks.

Unified login error messages

The aim of unifying the error messages shown during login attempts is to make it impossible to guess valid usernames.

ACCESS CREDENTIALS

Contact

For all registration-related requests, use the contact email address: registrace@czmvo.cz

Once CZMVO registers you in the Alert Management System, the system sends you an email with your access credentials.

Registration e-mail example

Note: Access credentials enable access to the production environment as well as the test or development environment.

Registration email example

From: NOOL <no-reply@czmvo.cz>
Date: Wednesday 12th July 2026 12:27
To whom: <info@czmvo.cz>
Subject: < CZMVS - registrace - sprava Alertu/CZMVS - registration - Alert administration >

Na tento e-mail neodpovidejte - je automaticky generovan systemem!/Do not reply to this e-mail - it is automatically generated by the system!

Vazeny pane/pani, zasilame Vam pristupy do NOOL IS:/Dear Sir/Madam, we send you access to the CZMVO IS:

Pristupove udaje/Access credentials:

Login: xxxx

Heslo/Password: yyyyyyyyyy

Pristupove udaje vlozte zde / Access credentials insert here:

https://portal.czmvo.cz/

Pro pristup do testovacího prostredi ci pro komunikaci pres API kontaktujte registrace@czmvo.cz / For Test environment or for API interface access please contact registrace@czmvo.cz

Platnost pristupovych udaju: 96 hodin (4 dny). / Validity of access credentials: 96 hours (4 days).

Velmi doporucujeme si **pristupove udaje po uspesnem prihlaseni zmenit.**

We strongly recommend that **you change your login credentials after successfully logging in**.

NOOL, z.s.

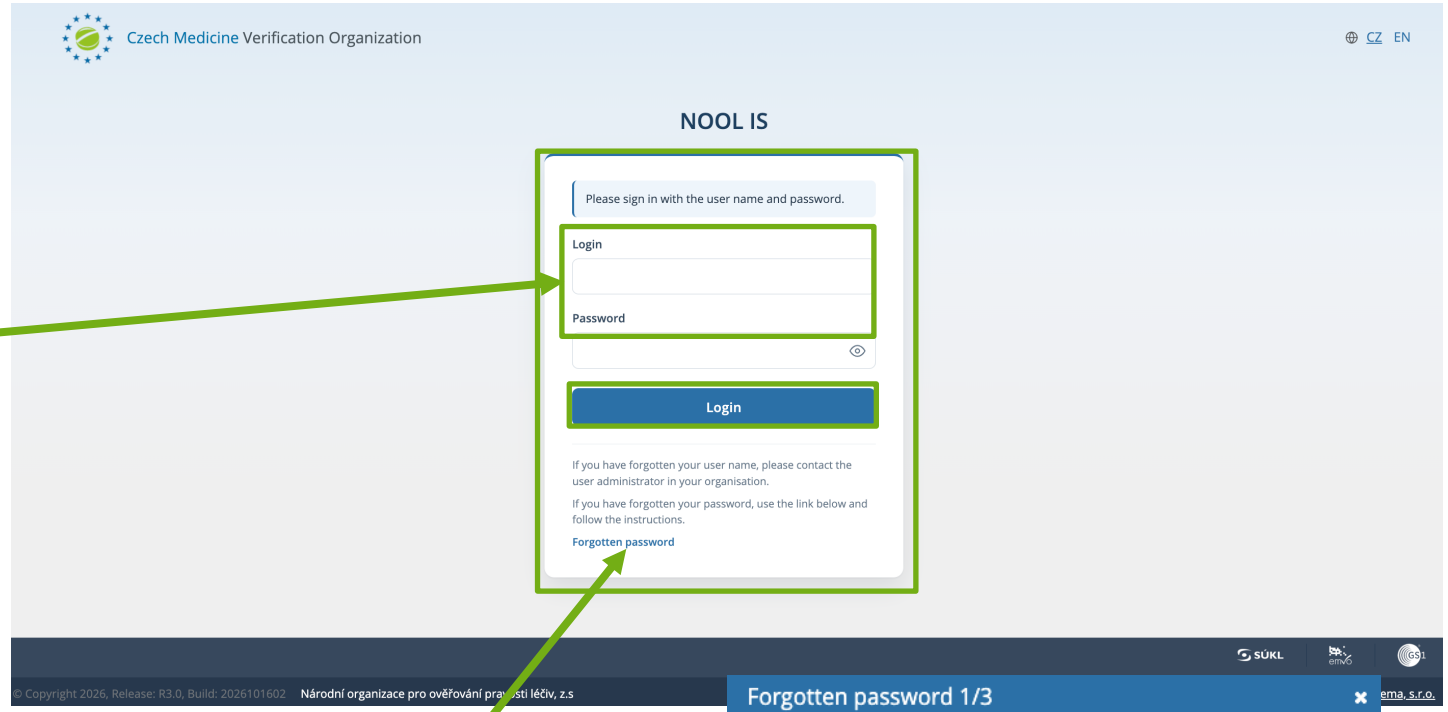
LOGGING IN TO THE ALERT MANAGEMENT SYSTEM

The web interface of the **PRODUCTION** Alert Management System is available at: https://portal.czmvo.cz/

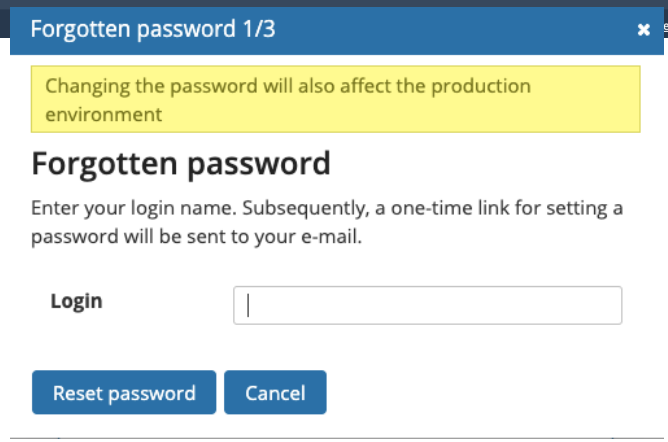
1. After entering the web address, the login dialog is displayed.
2. Enter your access credentials (login and password), and click „***Login***“.

The web interface of the **TEST** Alert Management System is available at: https://sandbox.czmvo.cz/. It is used for testing software for the current production environment and is functionally equivalent to the production environment. A copy of production data is uploaded to the test environment regularly every night. You can therefore test with actual user data. Changes made in the test environment do not affect the production database and may be changed freely. However, data is overwritten every night, which must be taken into account during testing.

The **DEVELOPMENT** environment is intended for IT companies to test and develop software for a CZAMS version that has not yet been deployed to production and test environments. https://beta.czmvo.cz//



Note: If you forget your password, click „***Forgotten password“*** to generate a new one. If you do not know your username (login), request a new password at mailto:registrace@czmvo.cz.

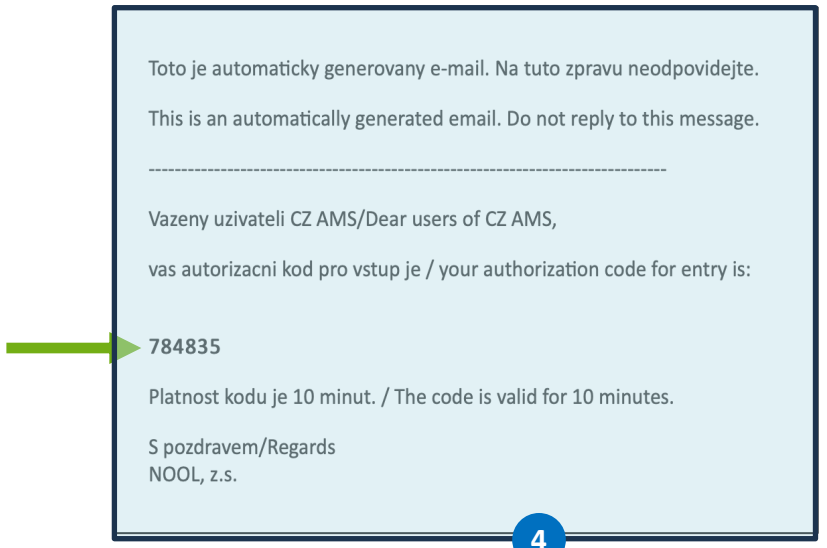


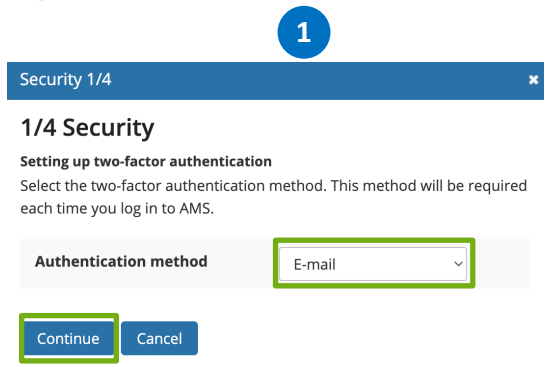
TWO-FACTOR AUTHENTICATION SETUP

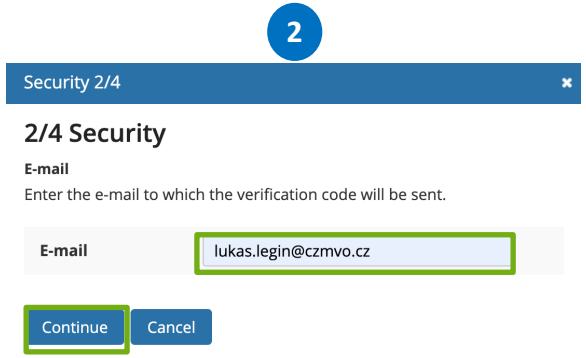
After successfully logging in to the web interface, you will be prompted to configure two-factor authentication. An email address or Google Authenticator can be selected as the second security factor.

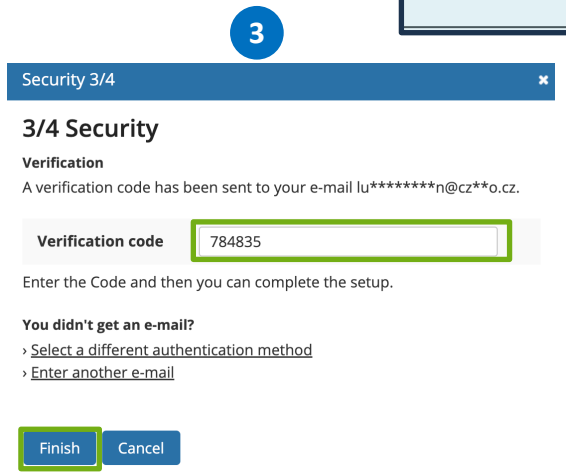
Setup using an e-mail address

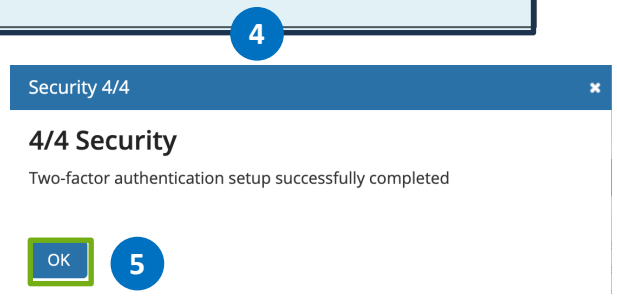
1. Select the **Email** verification method. Click "***Continue***".
2. Enter the email address to which the verification code will be sent in the **Email** field.
3. Copy the **authorisation code** from the email sent to the selected email address.
4. Enter the code in the **Verification code** field and click "***Finish***"
5. Click "***OK***". The setup is complete.









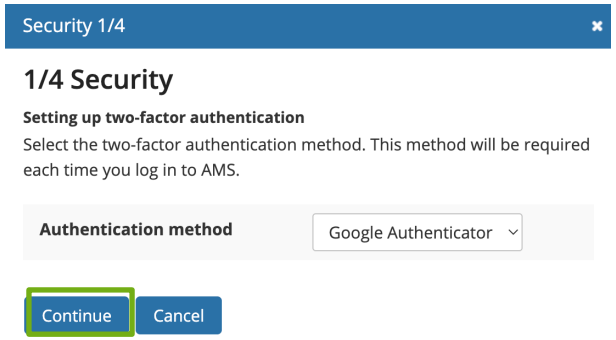


TWO-FACTOR AUTHENTICATION SETUP

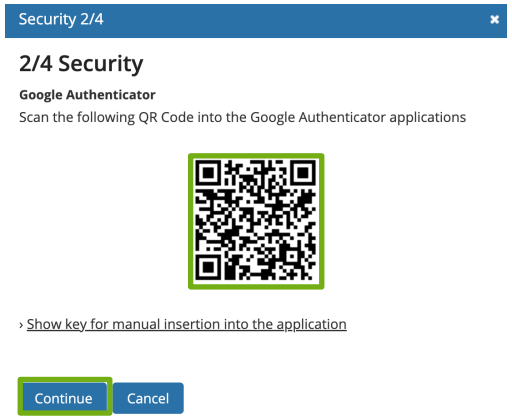
Setup using Google Authenticator:

1. Select the **Google Authenticator** verification method. Click "***Continue***".
2. Scan the **QR code** into the Google Authenticator application on your device.
3. Enter the current code shown in the application in the Verification code field and click "***Finish***".
4. Click "***OK***". The setup is complete.

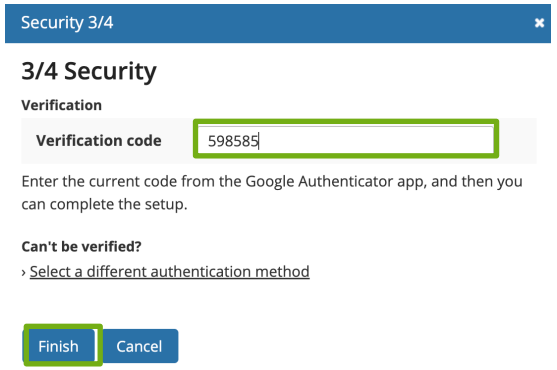
1



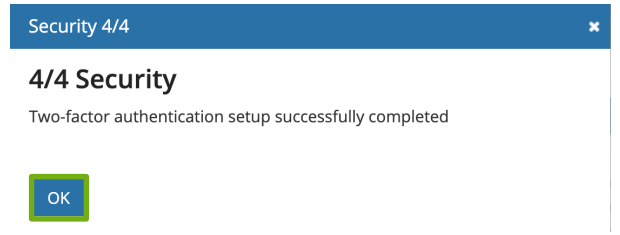
2



3



4



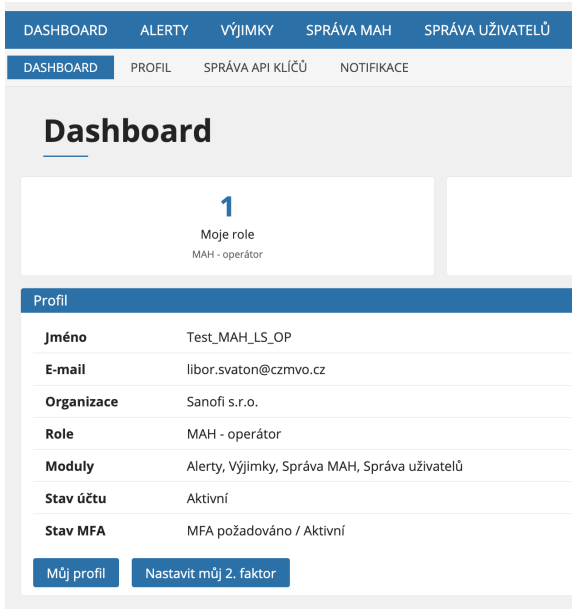
More information on using Google Authenticator is available on the provider's website: Google Authenticator

TWO-FACTOR AUTHENTICATION SETUP

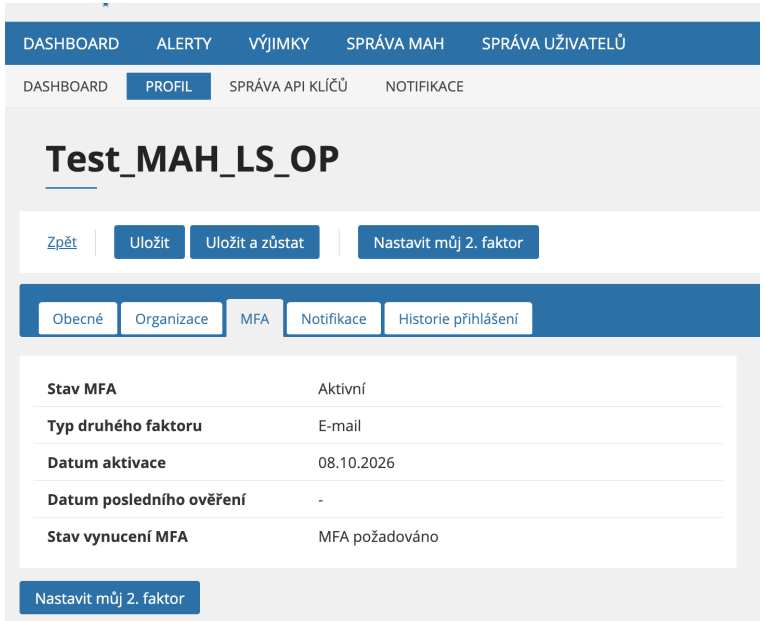
Depending on the selected verification method, you will be prompted to enter a verification code at each login, either by **email** or through **Google Authenticator**.

The two-factor authentication method can be changed at any time. There are several ways to change the settings. From the Main Menu, the easiest way is:

1. In the main menu, click “User Management” to open the “**Dashboard**”, then click “**Set up my second factor**” in the bottom-left corner.
2. Then follow the instructions on pages **11 and 12.**



Note:
You can also change your MFA settings by selecting “**User Management**”, then “**Profile**”, and finally “**Set up my second factor**”.
If you are already in your profile, you can also click “**MFA**”.
Then click “**Set up my second factor**” in the bottom-left corner.
Follow the instructions on pages 11 and 12.



MAIN MENU



1. Switch to **Dashboard** – an overview of outstanding requests, alert status and development, and other summary information.
2. Switch to the **Alerts** list – an overview of alerts and a workspace for investigating and closing alerts.
3. Switch to the **Exceptions** list – an overview of exceptions according to Ministry of Health and SIDC information (Section 11r, Section 13r, etc.).
4. Switch to **User Management** – available only to the organisation administrator; used to manage users, assign sites and manage notifications.
5. Switch to **End User Management**
6. Username
7. System-message indicator and access to the message list.
8. Security Management — select or change the **two-factor authentication method**

Change **password**

Language selection

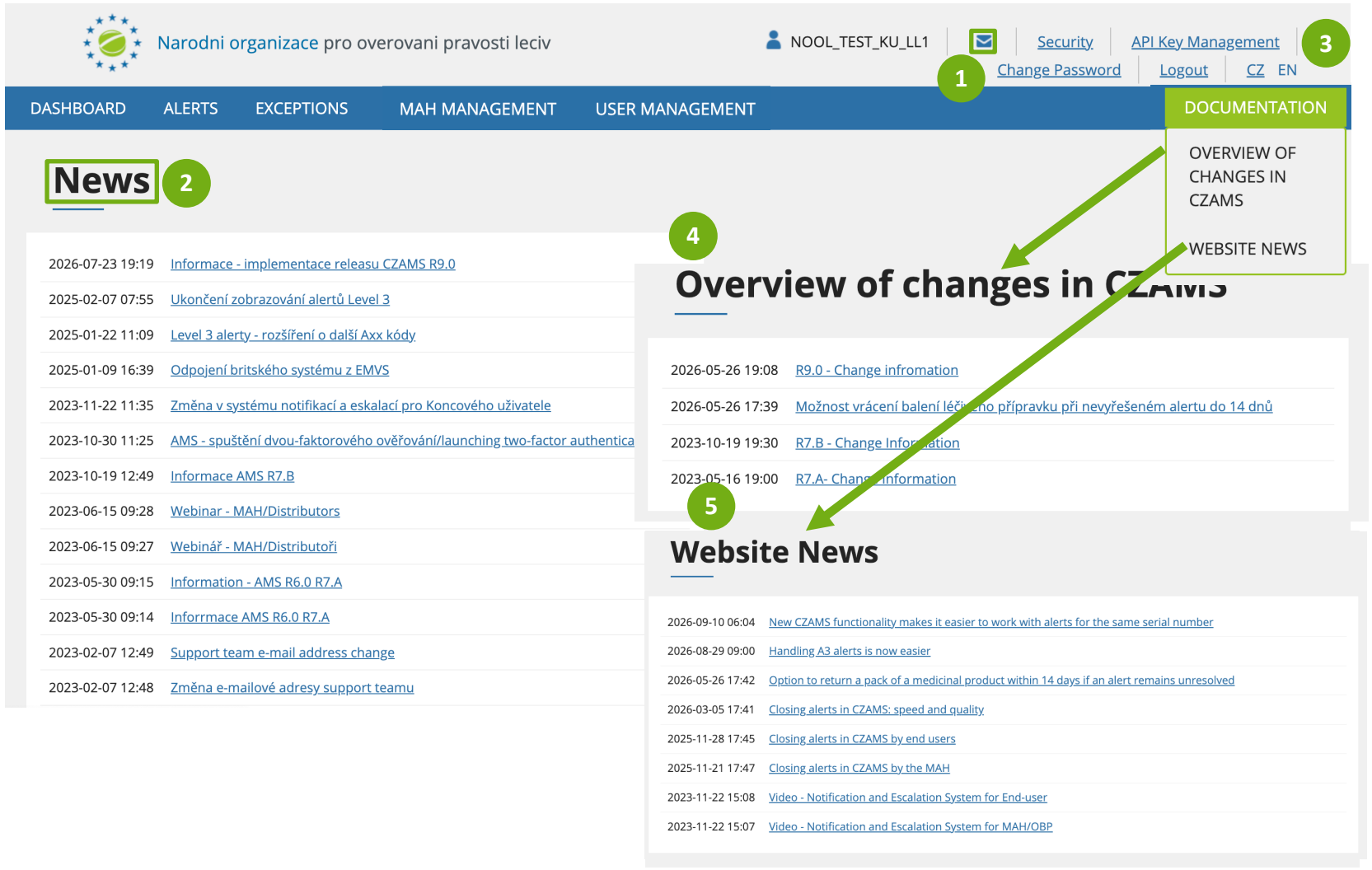
Link to an overview of **information on system changes** or important information on the CZMVO website.

INFORMATION ON CHANGES, NEWS AND NOTIFICATIONS

1 The top bar displays an "***Envelope***" showing the number of unread messages. Clicking 2 the envelope displays **the list of all messages. Unread messages are shown in bold**, while read messages are displayed in normal type. Once a message is read, the system stores information that it has been read by that particular user. 3

4 The **Documentation** option includes **Overview of changes in CZAMS**, containing links to the most important system changes. These most often relate to the implementation of a new release, but may also include other important announcements concerning system changes.

5 The **News** option contains text links to selected news items from the CZMVO website, for example "Did you know?".



DASHBOARD

After selecting Dashboard, you can choose between two modes: „**Requests**“ and „**Alerts**“.

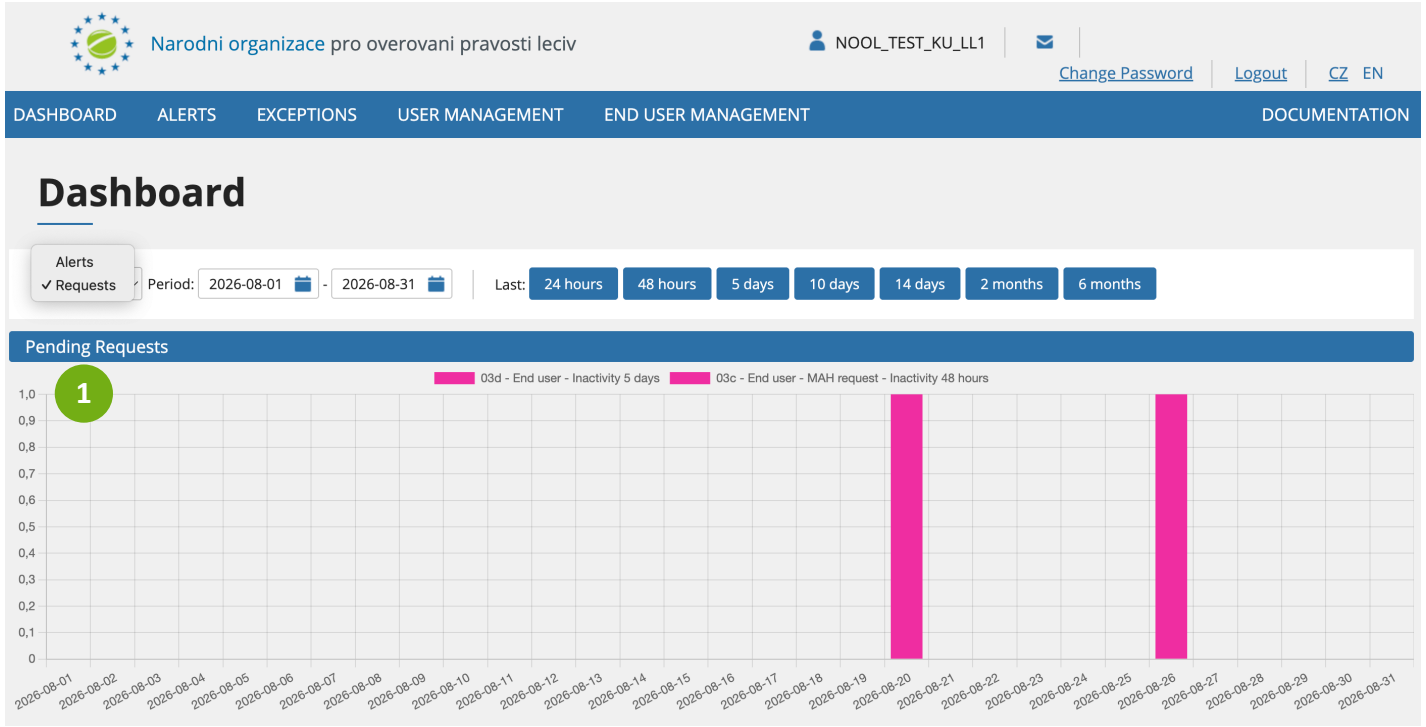
By default, the „**Requests**“ dashboard is displayed with information about **outstanding requests.**

It displays:

a) **A bar chart of outstanding requests** for the selected period by current status. 1

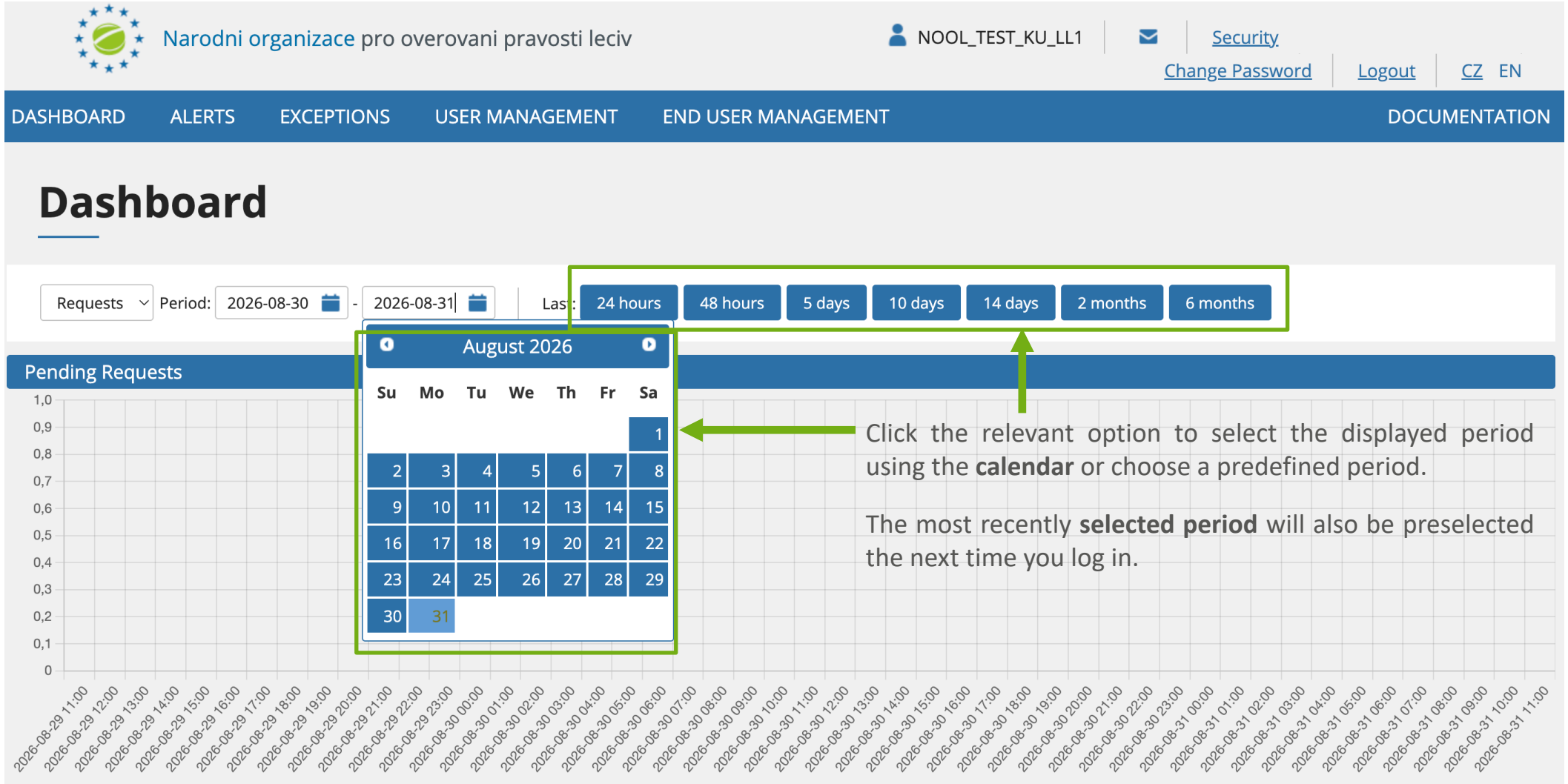
b) **Pie charts** with information for the selected period**:**

- ✓ Summary information with a direct link to the selected group 2
- ✓ Number of active MAHs and end users in the CZMVO information 3
- ✓ Open alerts 4
- ✓ Outstanding requests by status 5

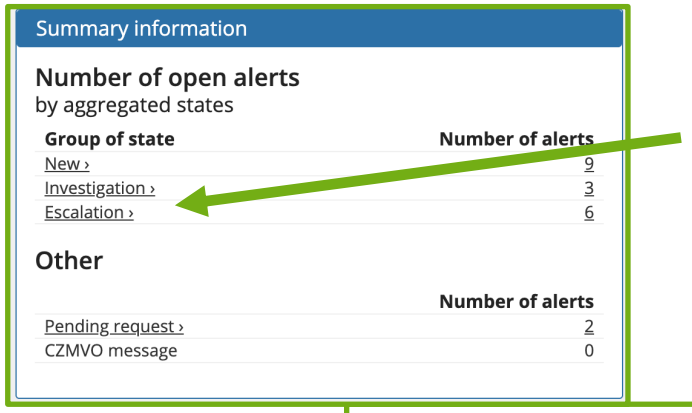


Use the „**Show values**“ switch to display a table of absolute values.

DASHBOARD

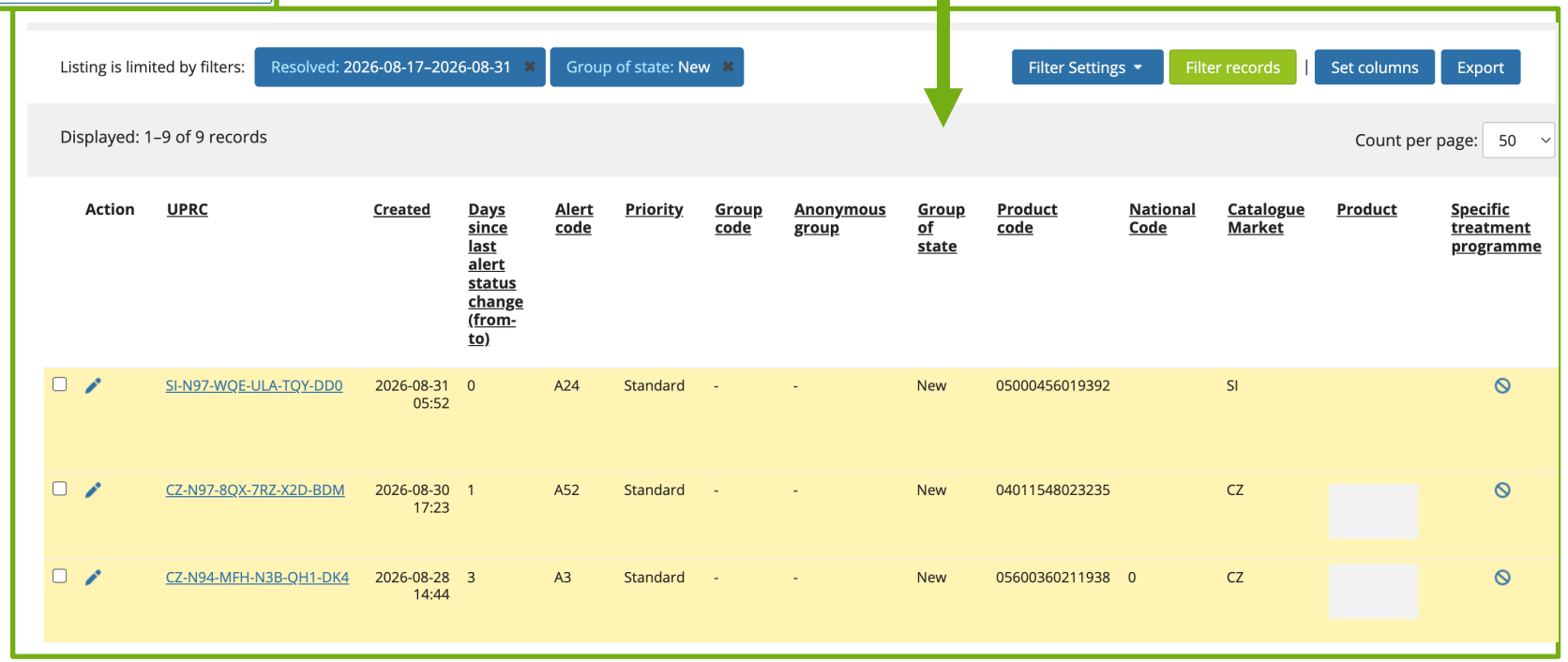

Narodni organizace pro overovani pravosti leciv
NOOL_TEST_KU_LL1
Security
Change Password
Logout
CZ EN
DASHBOARD
ALERTS
EXCEPTIONS
USER MANAGEMENT
END USER MANAGEMENT
DOCUMENTATION
Dashboard
Requests
Period:
2026-08-30
2026-08-31
Last:
24 hours
48 hours
5 days
10 days
14 days
2 months
6 months
August 2026
Su Mo Tu We Th Fr Sa
Pending Requests
Click the relevant option to select the displayed period using the calendar or choose a predefined period.
The most recently selected period will also be preselected the next time you log in.

DASHBOARD



The **Summary information** table displays an overview of alerts in the „**New**“ and „**Investigation**“ statuses and the number of outstanding requests or received messages.

Clicking an alert status, or a number in the relevant row, opens the list of all alerts in that status and period. This provides a direct link to the „**Alerts**“ tab with a filter preset according to the request in the **Summary information** table and the **selected period**.



DASHBOARD

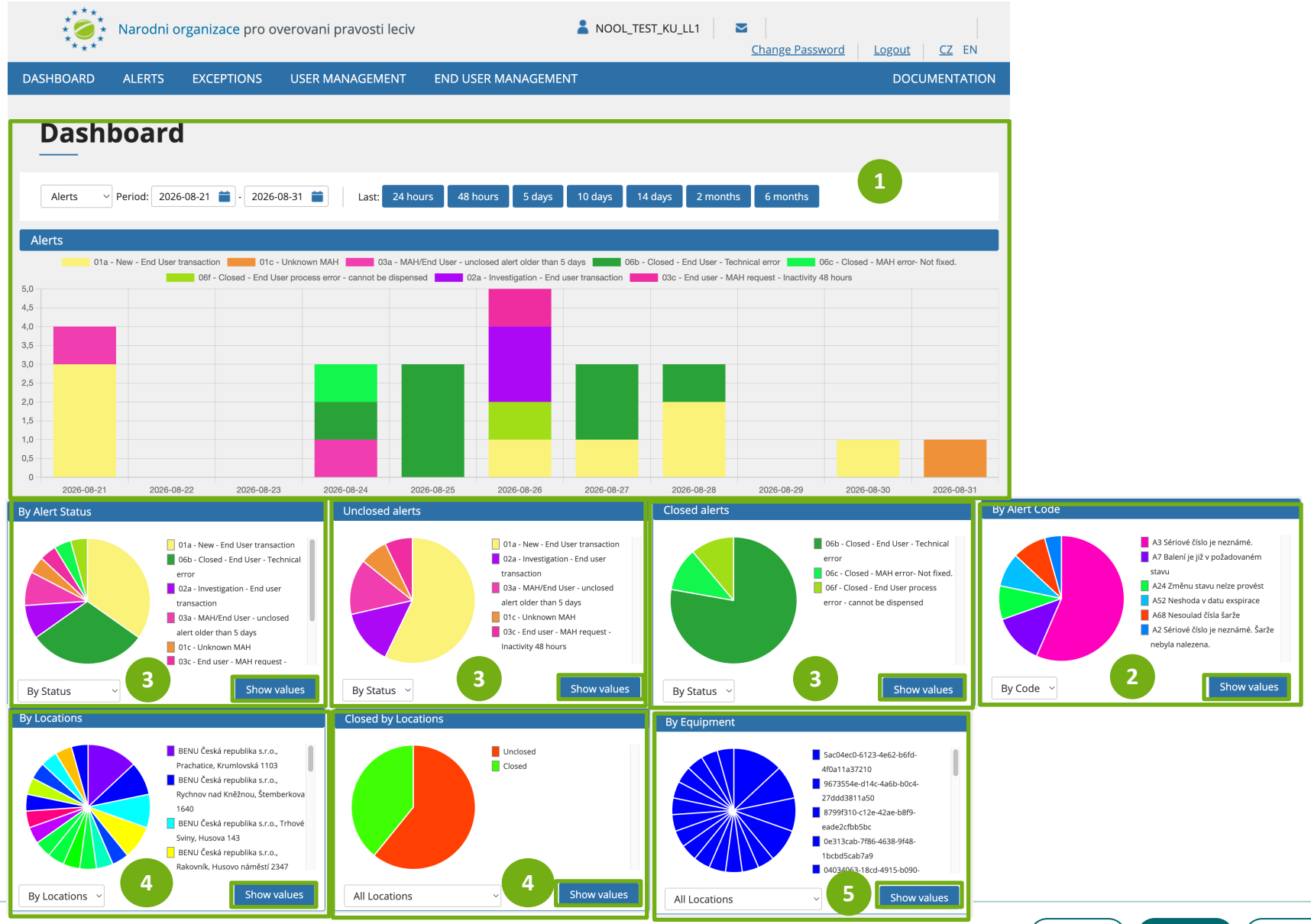
After selecting „**Alerts**“, the dashboard displays:

a)A **bar chart** of alerts generated during the selected period by current status. 1

b)**Pie charts** with alert information for the selected period: 2

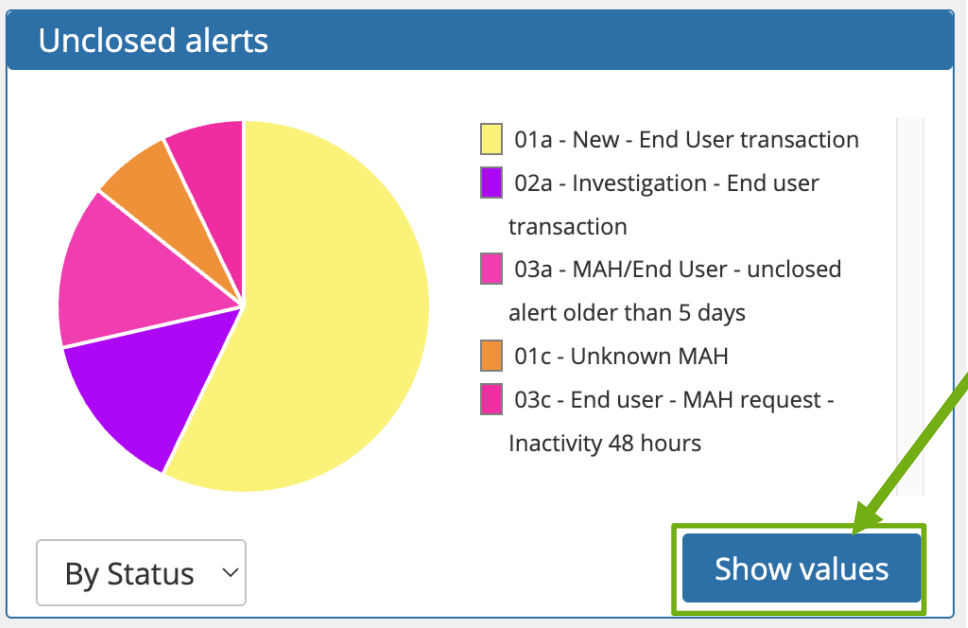
- ✓ By alert code 3
- ✓ By alert status 4
- ✓ By locations within the organisation 5
- ✓ By individual devices within the organisation.

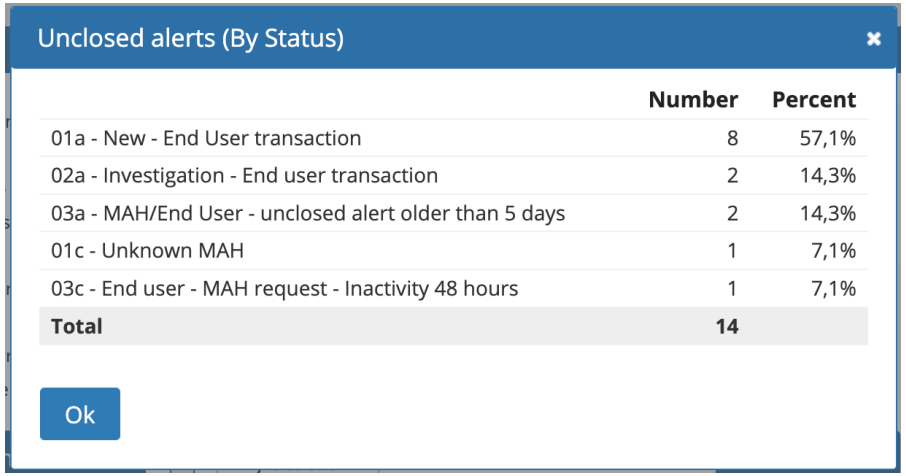
Use the „**By status / By code / By location**“ switch to change the data source. Use „**Show values**“ to display a table of absolute values.



DASHBOARD

In all tiles with pie charts, click „**Show values**“ to display the absolute values and percentage distribution for the relevant pie chart





Part II

User Management

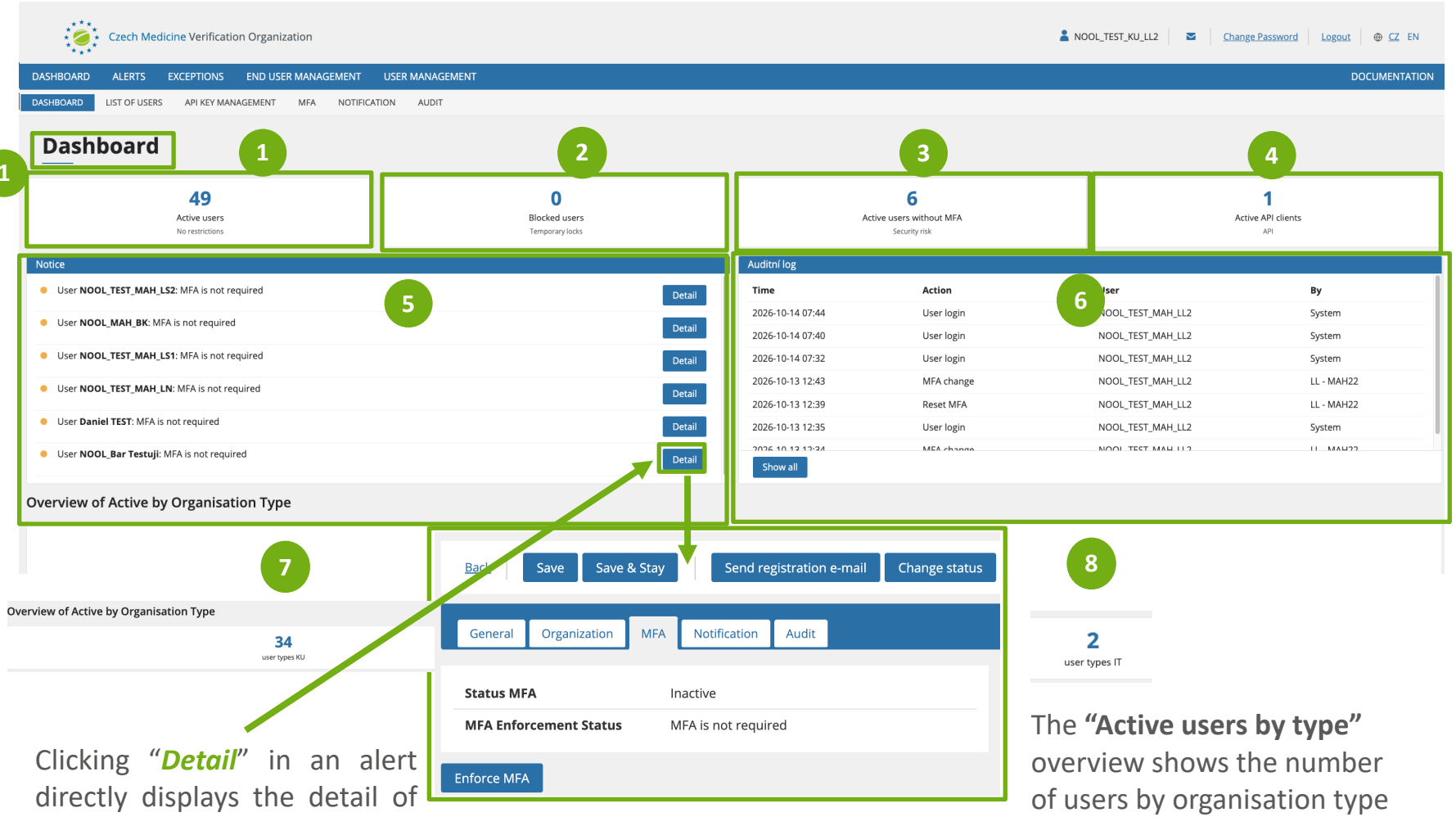
USER MANAGEMENT - DASHBOARD

In the "**User Management**" section, the default view is the "**Dashboard**" sub-option.

It shows information on the total number of **active users within the organisation**, the number of **blocked users,** the number of **active users without MFA** set up and, where applicable, **the number of active users connected via the API.**

The "**Notice**" section shows a list of users that probably need to be dealt with.

The "**Audit log**" section shows user activities in the system.



Clicking "***Detail***" in an alert directly displays the detail of the specific user, so that it can be dealt with immediately.

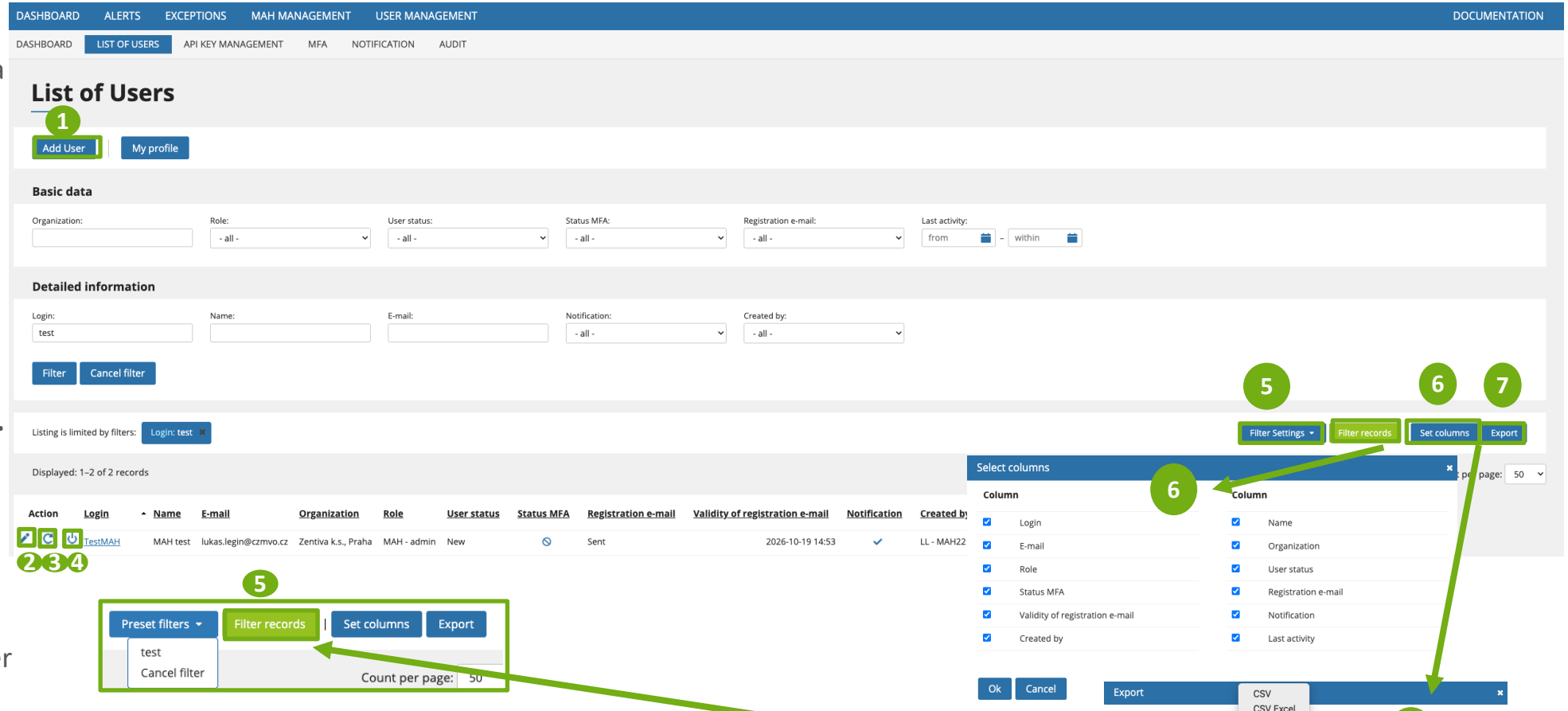
The **"Active users by type"** overview shows the number of users by organisation type (End User, IT Company).

USER MANAGEMENT – USER LIST

In the "**User Management**" section, a user with the "**Administrator**" permission can:

1. ✓ **create new users,**
2. ✓ **edit them,**
3. ✓ **set up MFA,**
4. ✓ **change their status.**

Users with other permissions do not have access to this section.



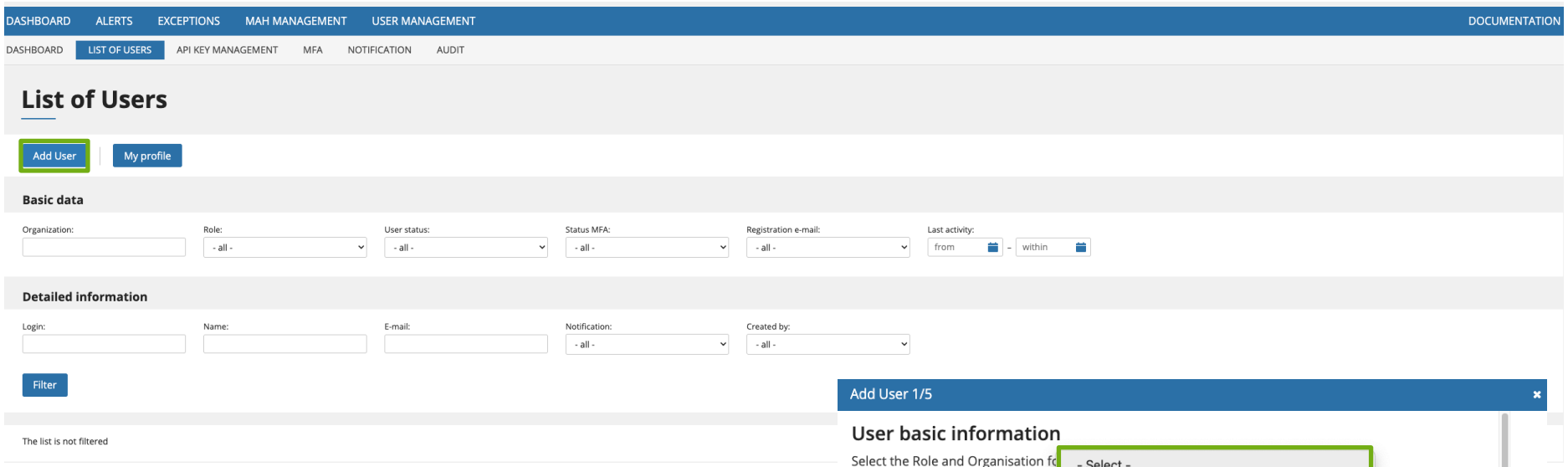
PERMISSIONS:
MAH administrator – user management, full alert management,
MAH operator – full alert management,
MAH viewer – viewing and outputs only.

In "User Management", users can be **searched for and sorted using filters** 5 (more about working with filters in section "Alerts – Filters"), the 6 **columns in the list can be set,** 7 and **data can be exported** to CSV or XLSX as selected (all, a selection of data groups, the currently selected columns).

USER MANAGEMENT – ADDING A USER

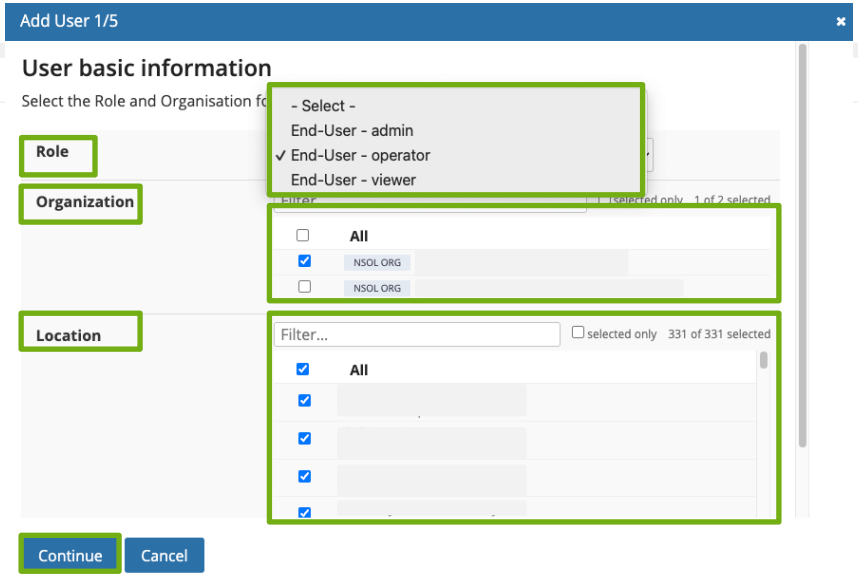
A new user is added by clicking "**Add user**" in five steps:

1. Entering the user's basic details (role, organisation).
2. Entering the login details (login, name, e-mail).
3. Setting up MFA and notifications.
4. Checking the details.
5. Confirming and creating the new user.



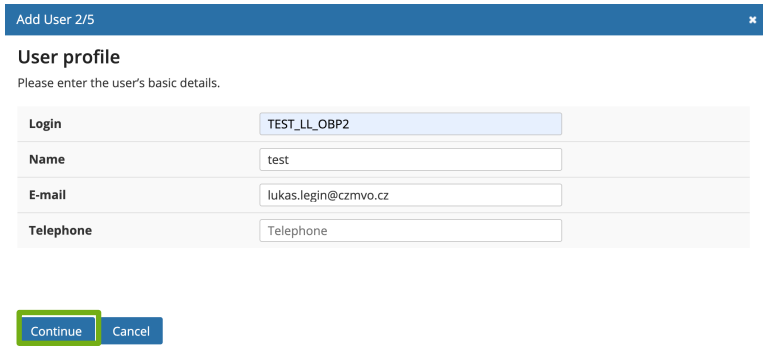
Select the new user's "Role" and assign them to an "Organisation/s and Locations". If an Organization or a Location is missing from the list, contact suport@czmvo.cz. Click "Continue".

- Note: A user can manage the alerts not only of one organisation but of several Organizations, including all or selected Locations.



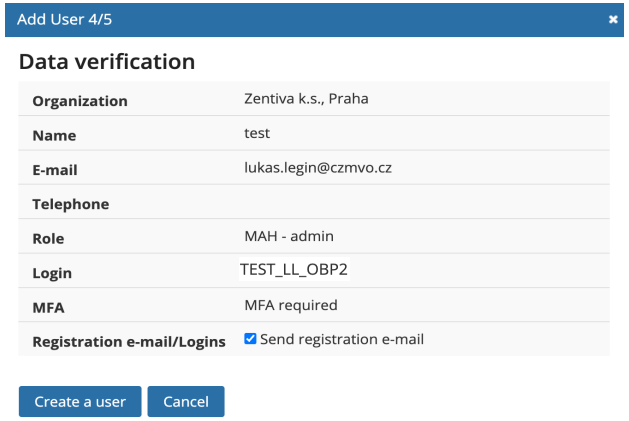
USER MANAGEMENT – ADDING A USER

2



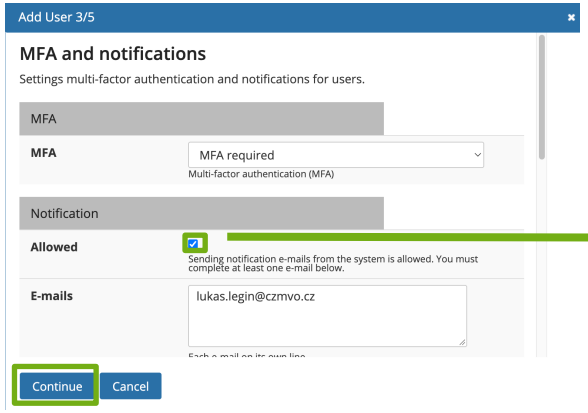
Enter the **user profile** (login, name, e-mail, optionally a telephone number). Click "**Continue**"

4



Check the details for the new user. If everything is correct, click "**Create user**".

3

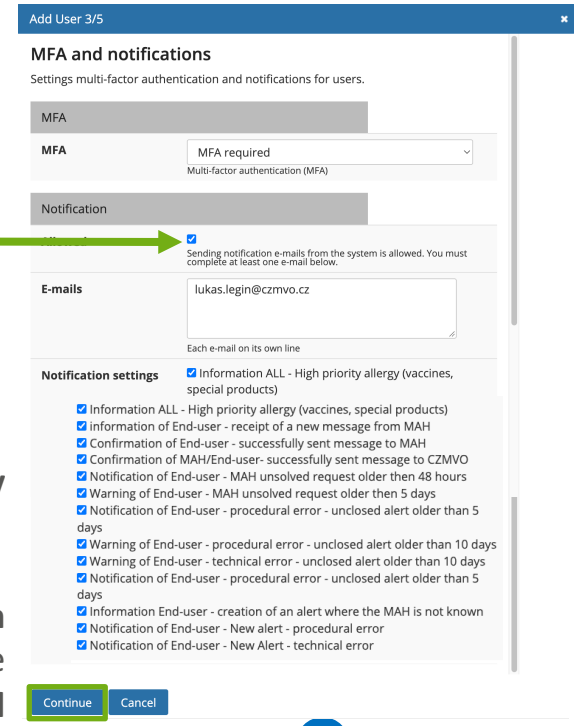


Set up MFA – MFA is always **mandatory** except for the MAH viewer role.

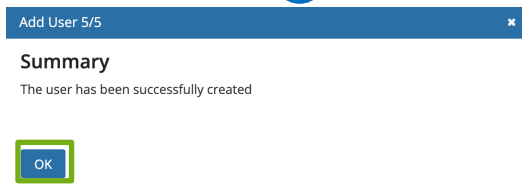
If you want the user to receive **system notifications**, tick the "**Allowed**" box in the "**Notifications**" section. The **contact e-mail** is pre-filled (it can be changed), and further e-mails can be added (each e-mail on a separate line), together with **all notifications available to the given role**. You can cancel them by unticking them.

Caution! Within the Organisation, there must be at least one user receiving each notification. Then click "**Continue**".

3



5



After **confirming** with "**OK**", the new user is created and a **registration e-mail** is sent to them at the same time.

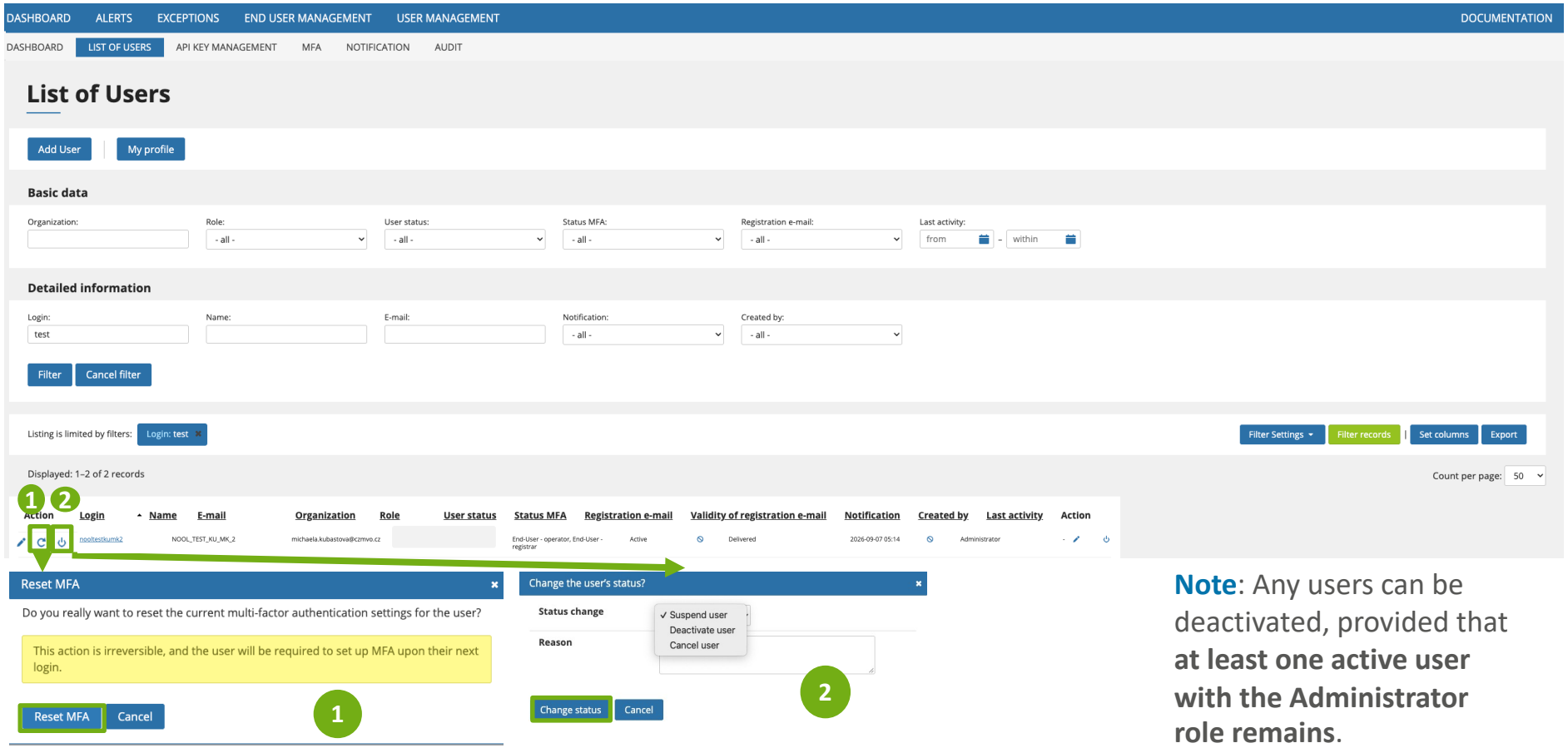
USER MANAGEMENT – EDITING A USER

1 Changes to MFA settings

Clicking the "**refresh**" icon displays a prompt asking whether you really want to cancel the current MFA settings. If you click "**Reset MFA**", the user will have to set up MFA again the next time they log in. This function can be used, if there are problems with sending the second access codes.

2 Changing the user status

is used when the Organisation's admin temporarily suspends a user's access or wants to deactivate or cancel the user completely. A user can also be unblocked here if they have repeatedly (3×) entered an incorrect login or password. The status is changed by clicking the "**power**" icon.



Note: Any users can be deactivated, provided that **at least one active user with the Administrator role remains**.

USER STATUSES: **NEW –** newly created, awaiting confirmation of the registration e-mail
EXPIRED – the user did not register within 96 hours (4 days)
BLOCKED – the user repeatedly entered an incorrect login or password
SUSPENDED – user suspended by the administrator; can be activated
DEACTIVATED – inactive user; can be reactivated
CANCELLED – cannot be reactivated; kept in the archive for 7 years, then irreversibly deleted

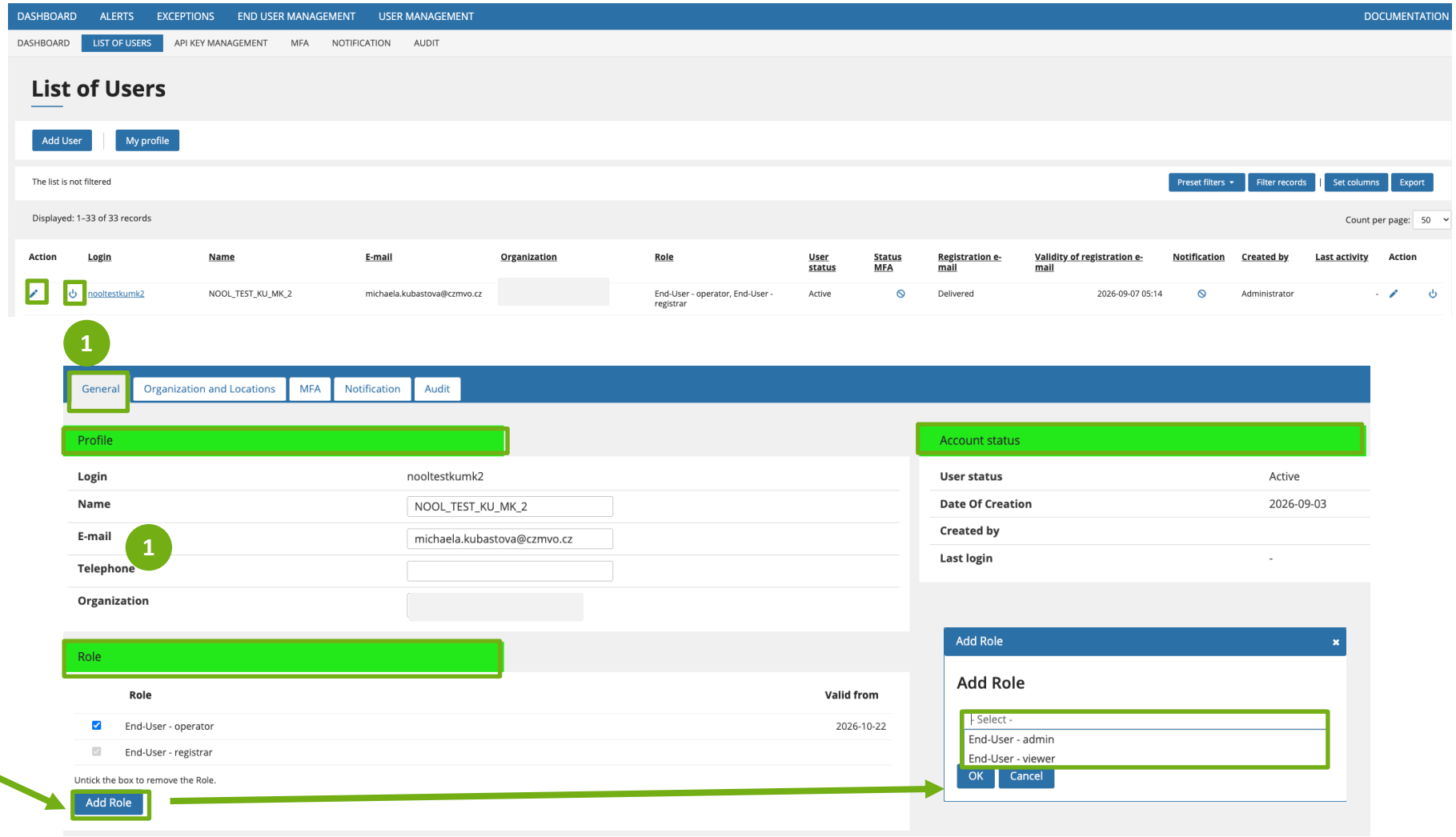
USER MANAGEMENT – EDITING A USER

Clicking the "**pencil**" icon or the "**Login name**" in the User list opens the user detail.

It contains **six** tabs in total: "**General**", "**Organisation**", "**MFA**", "**Notifications**", "**Login history**" and "**Audit**".

The 1 "**General**" tab shows the user's basic details, their role and the account status.

The role can be modified (added, removed, changed) by clicking "Add role".

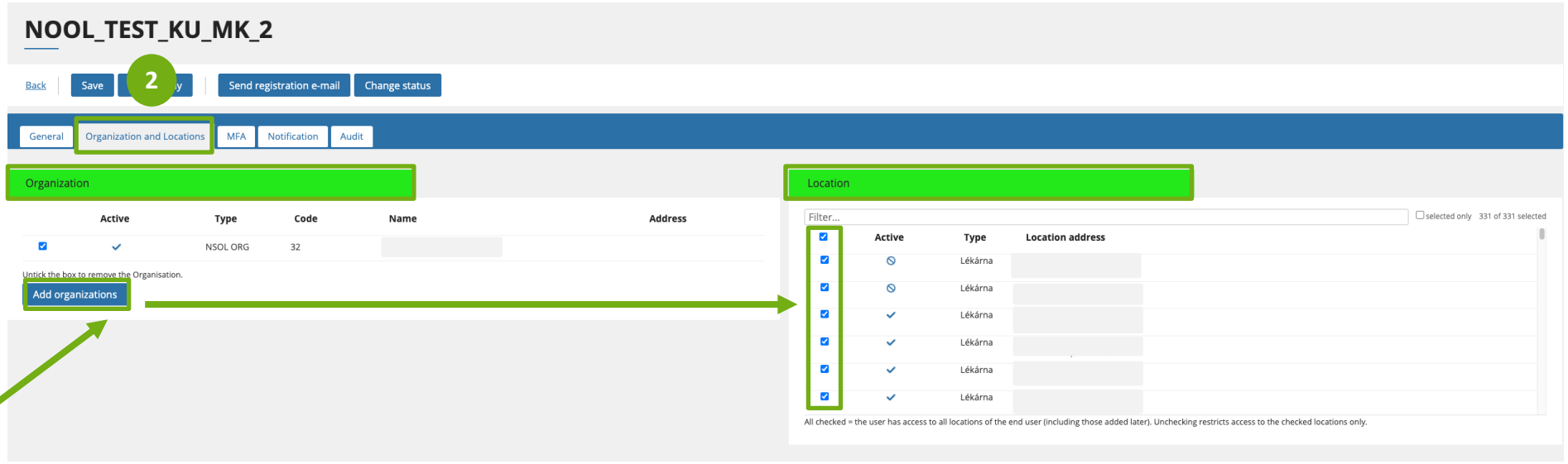


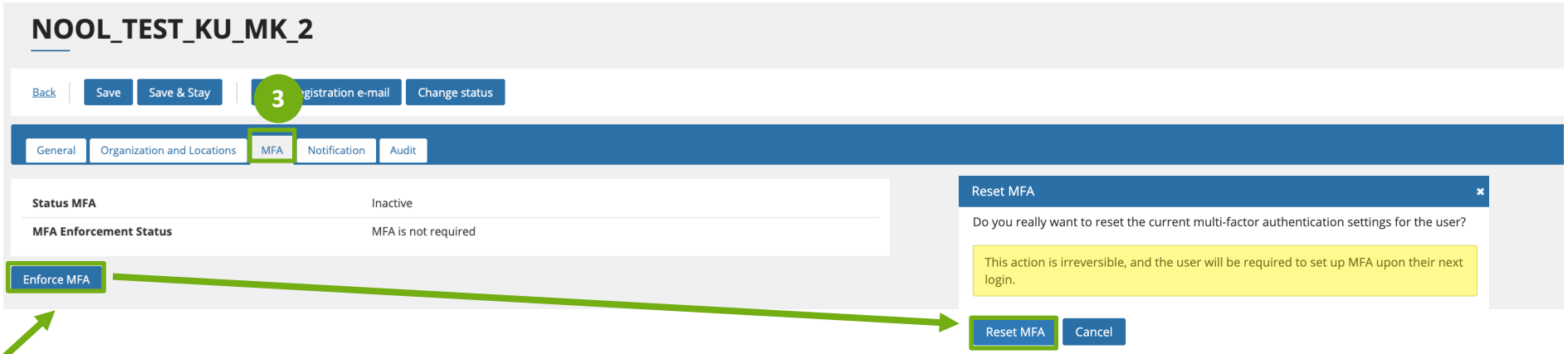
USER MANAGEMENT – EDITING A USER

The 2 "**Organisations and Locations**" tab shows the basic details of the Organisation(s) within which the user can operate.

The list of Organisations an locations can be modified (added, removed, changed) by clicking/ unclicking "**Add organisation**".

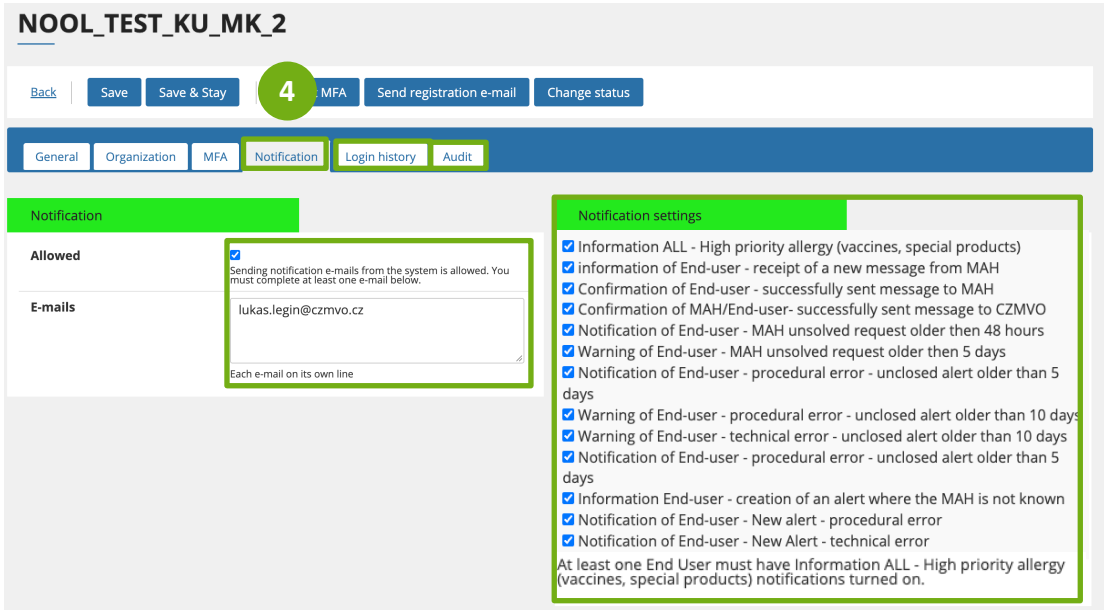
The "**MFA**" 3 tab shows the status and type of the second authorisation factor and whether MFA is required or not required (only in exceptional cases). Clicking "**Reset MFA**" deletes the MFA settings, forcing the user to **set up MFA again.**





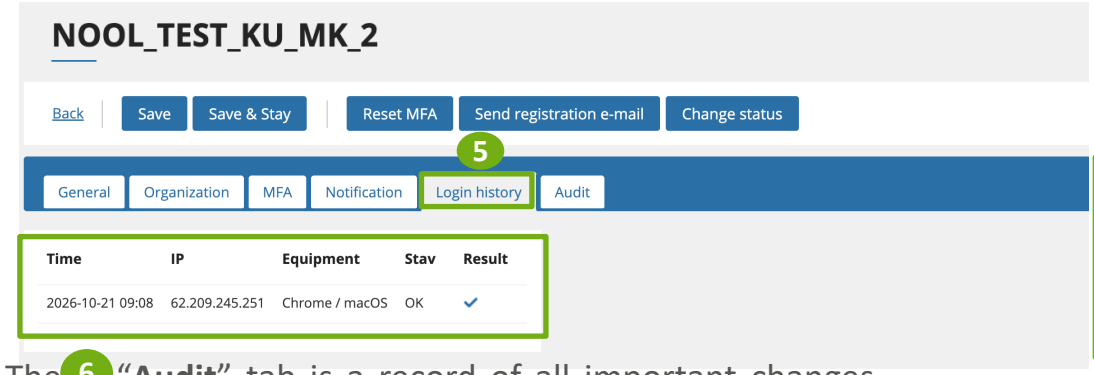
USER MANAGEMENT – EDITING A USER

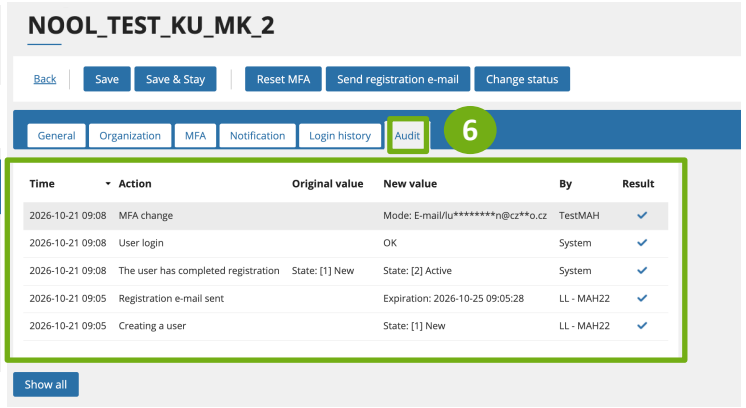
The 4 "**Notifications**" tab shows whether and which notifications are active for the given user. It also shows the e-mails to which notifications are sent (this is also possible for persons who are not NOOL IS users). The list of notifications and the notification e-mails can be modified as needed.



Note: If sending notifications is enabled, at least one notification e-mail must be filled in.

The 5 "**Login history**" tab is a record about the user: from which IP address they logged in, when, and from which operating system and browser.





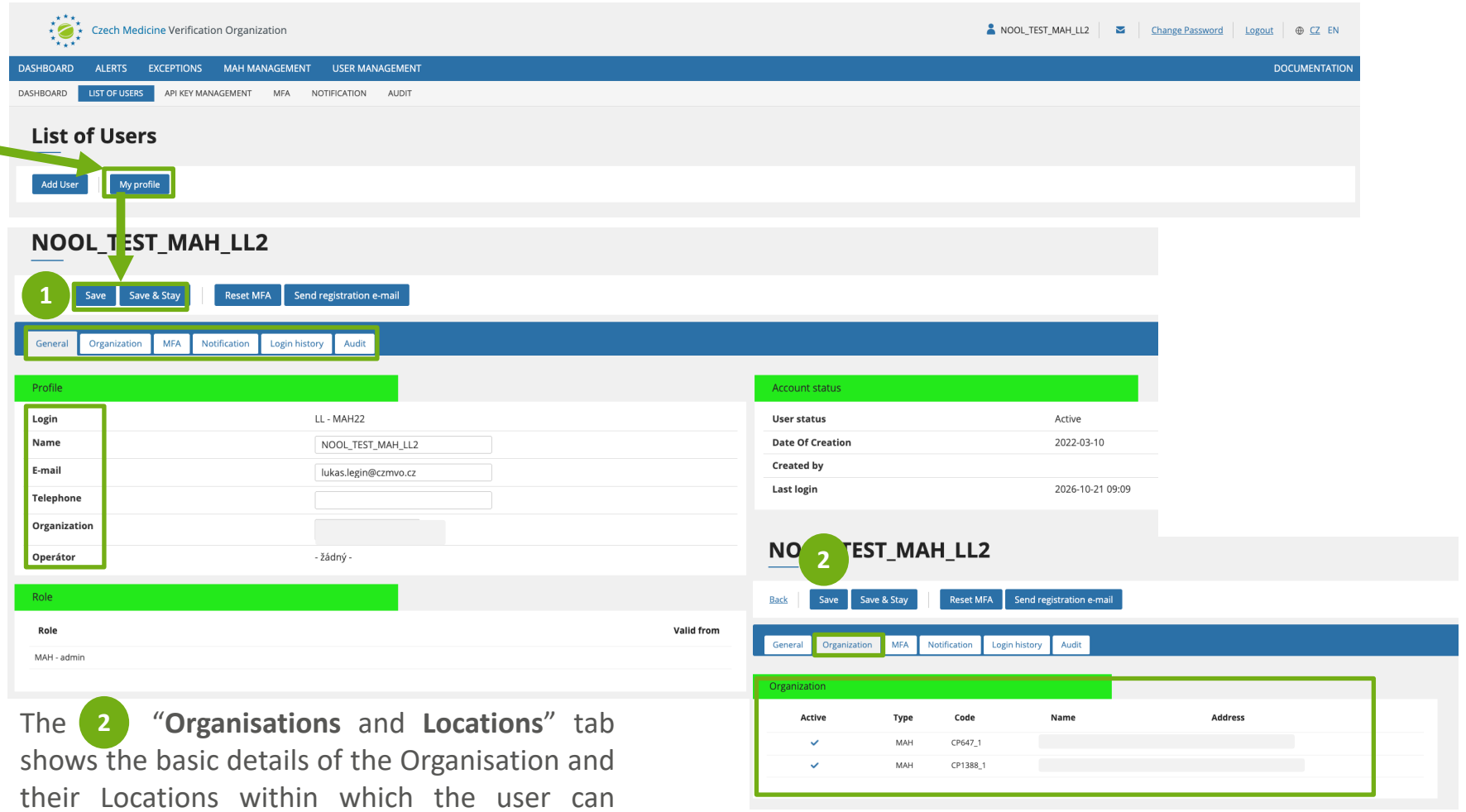
The 6 "**Audit**" tab is a record of all important changes made in relation to the given user (registration statuses, status changes, MFA changes, etc.).

USER MANAGEMENT – MY PROFILE

In the user list, you can **quickly obtain information about your account settings** by clicking "**My profile**"

The **detail of your profile** is displayed with six tabs containing all information about the profile; some of it can also be edited here.

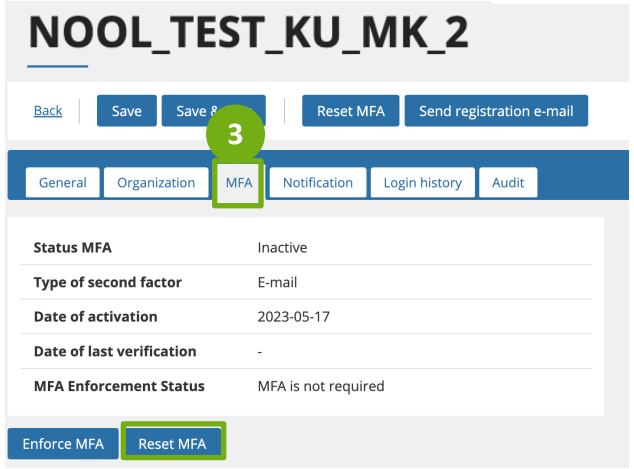
The 1 "**General**" tab shows the user's basic details, their role and the account status. Here you can change the "Name", "E-mail" and "Telephone". If you have the "Admin" permission, you can also modify the **list of Organisations** and **Locations** whose alerts you will have access to. Save the changes by clicking "**Save**" or "**Save and stay**".



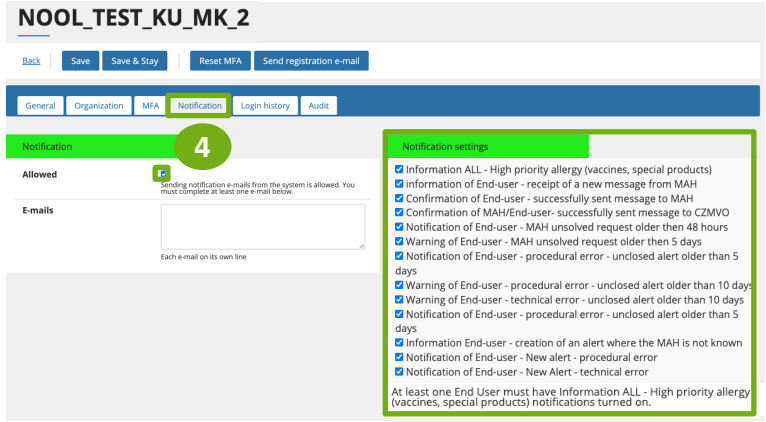
The 2 "**Organisations** and **Locations**" tab shows the basic details of the Organisation and their Locations within which the user can operate.

USER MANAGEMENT – MY PROFILE

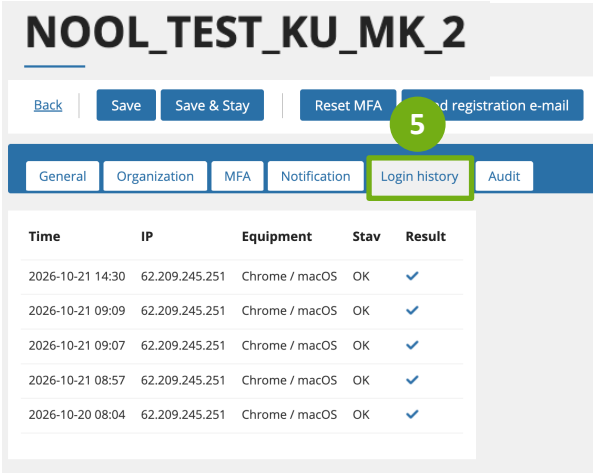
The 3 "MFA" tab shows the status and type of the second authorisation factor and whether MFA is required or not required (only in exceptional cases). Clicking "**Reset MFA**" deletes the MFA settings, forcing the user to set up MFA again.



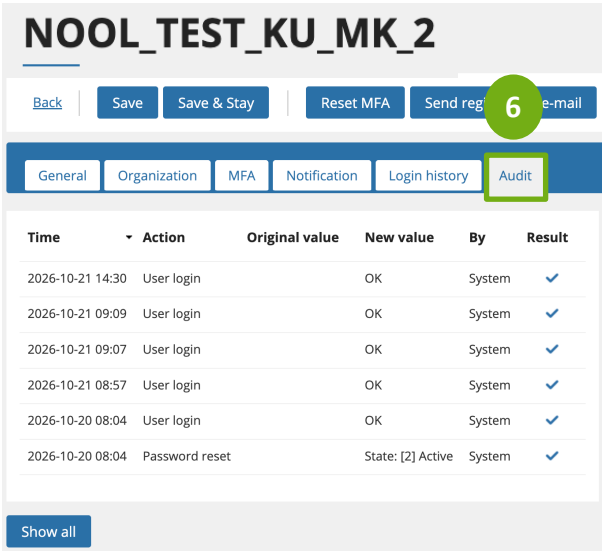
The 4 "**Notifications**" tab shows whether and which notifications are active in your account. It also shows the e-mails to which notifications are sent (this is also possible for persons who are not NOOL IS users). The list of notifications and the notification e-mails can be modified as needed. Note: If sending notifications is enabled, at least one notification e-mail must be filled in



The 5 "**Login history**" tab is a record about the user: from which IP address they logged in, when, and from which operating system and browser.

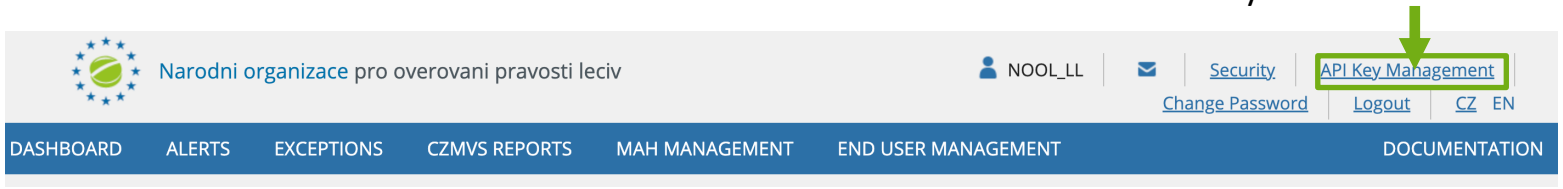


The 6 "**Audit**" tab is a record of all important changes made for the given profile (registration statuses, status changes, MFA changes, etc.).

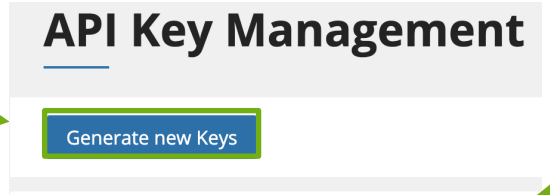


API KEY SETUP FOR COMMUNICATION WITH CZAMS

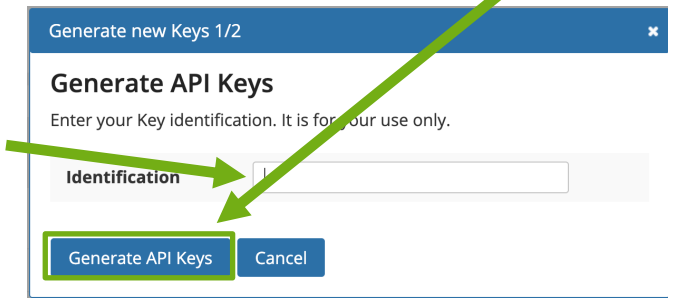
For API communication, generate the credentials in API Key Management: Client ID and Client Secret Key. These credentials are used by your application to authenticate API communication with CZAMS.
Do not confuse the Client ID with the location or device identifiers in CZMVS. Treat the Client Secret Key as confidential.



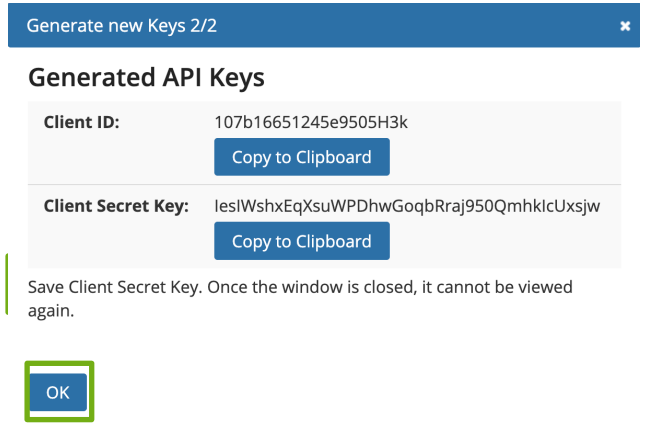
1. In API Key Management, select "Generate new keys".



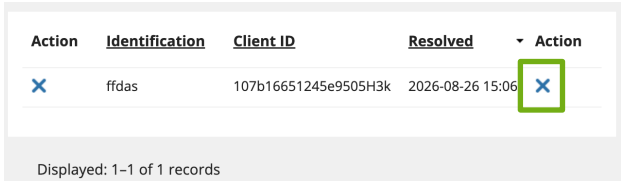
2. Enter a descriptive name for the credentials, for example "My API key".



3. After selecting „Generate API keys" the API key values will appear. Use the copy-to-clipboard button and save the credentials securely. These keys will be inserted into your application. Confirm by clicking „OK"

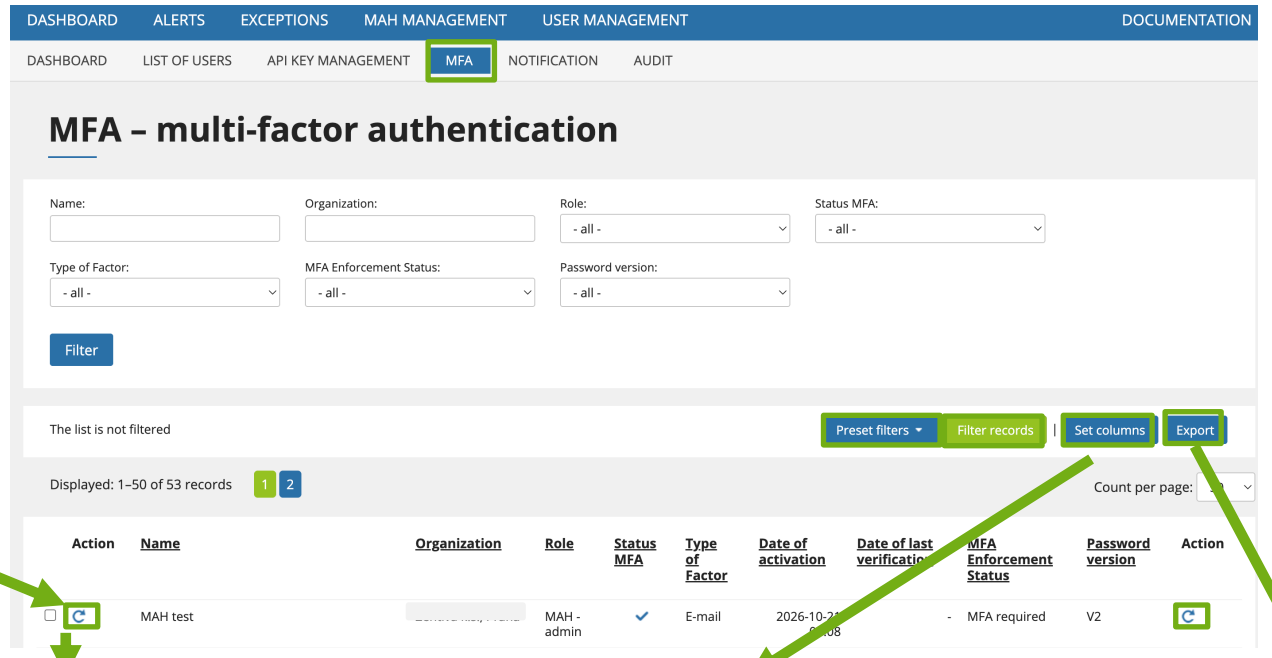


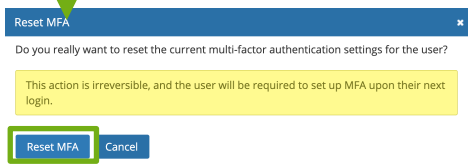
In „API Key Management" you can view your valid keys. Each key can be removed by clicking the „x" icon..

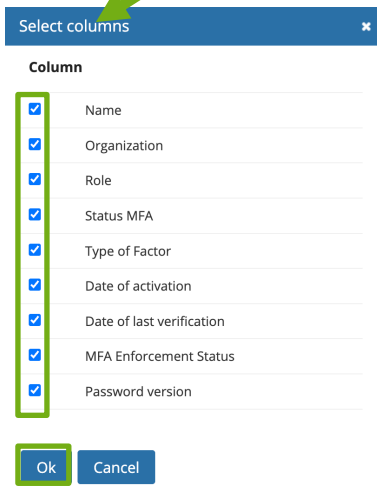


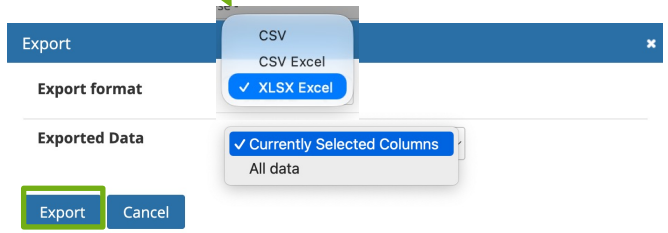
USER MANAGEMENT – MULTI-FACTOR AUTHENTICATION

The "**MFA**" tab shows an overview of all users and the **status and type of their second authorisation factor**. In the list, you can **set** the required **columns**, work with **filters** and **export** the data (CSV, Excel). Clicking the "**spiral**" icon next to a given user **forces MFA to be set up again** after confirmation by clicking "**Reset MFA**" („Resetovat MFA"). This action can also be **performed in bulk** after selecting (ticking) the request for selected (or all) users "**Enforce MFA**".











USER MANAGEMENT – NOTIFICATIONS

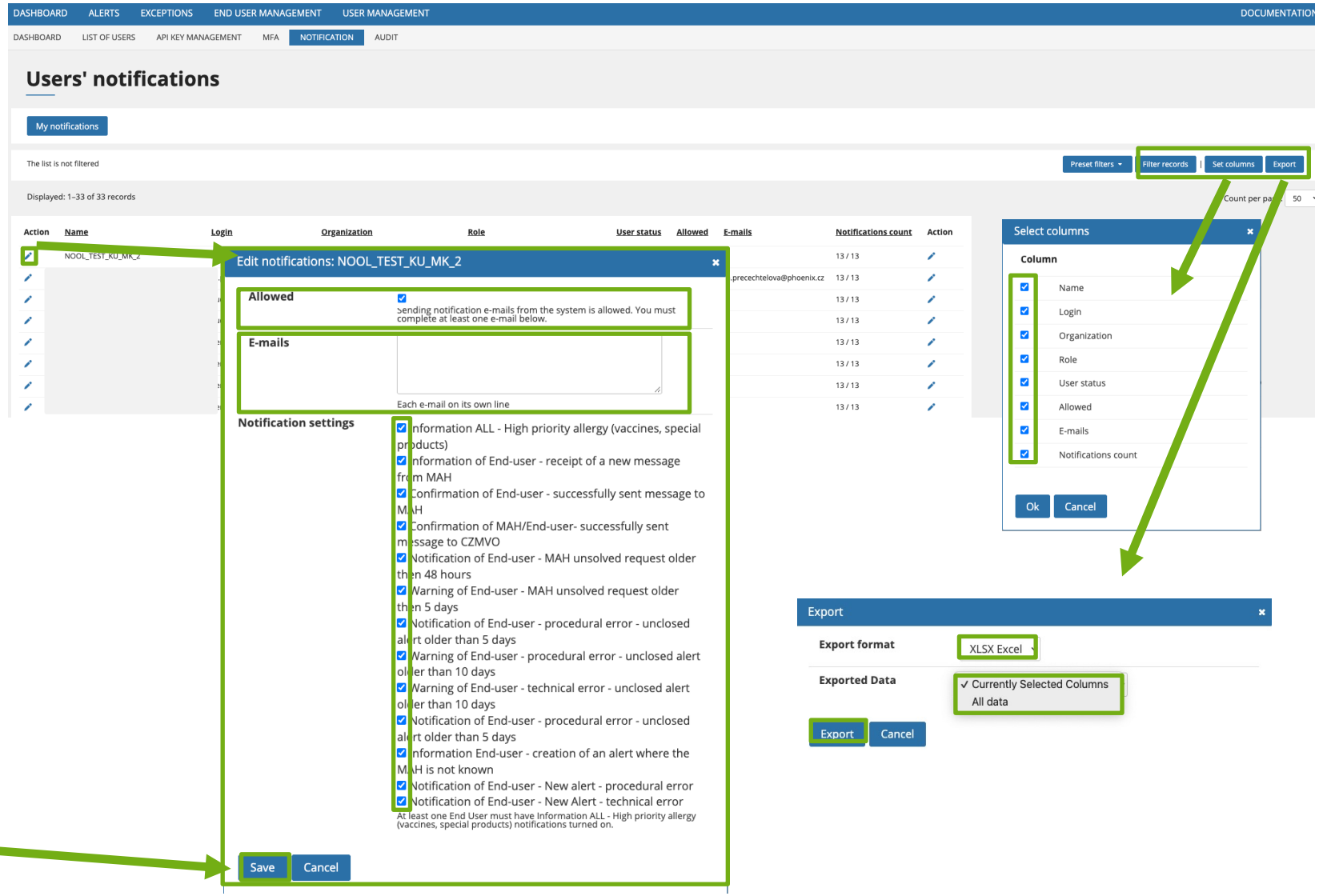
The "**Notifications**" tab displays a **list of users and their notifications**. You can **configure** the displayed **columns**, use **filters** and **export** the data to CSV or Excel.

Click **the pencil icon** next to a user to view their notification settings. The email addresses to which notifications are sent are also displayed.

A user with administrator permissions can enable or disable notifications and change the notification email addresses for individual users as required.

Note: If notifications are enabled, at least one notification email address must be entered. In addition, at least one user must have notifications of high-priority alerts enabled *("Information ALL — High-priority alert generated (vaccines, special products)").*

Click "**Save**" to save the changes.

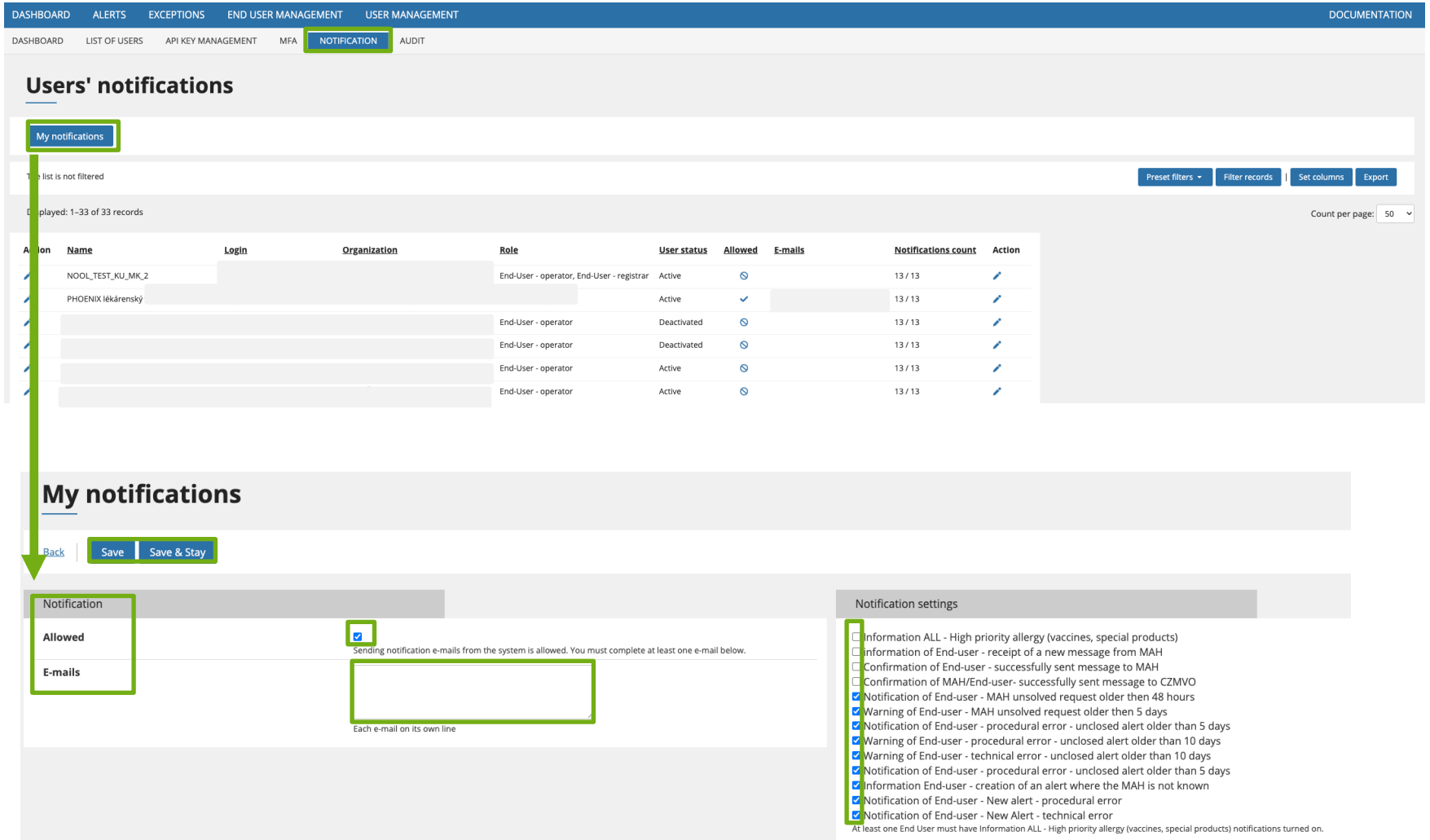


USER MANAGEMENT – NOTIFICATIONS

In the user list, click "**My notifications**" to quickly view the notification settings for your own account.

Your profile details are displayed, showing whether email notifications are enabled or disabled.

Here, you can add or remove the notifications you wish to receive and enable or disable notification delivery. You can also edit, add or remove notification email addresses. Click "**Save**" or "**Save and stay**" to save your changes

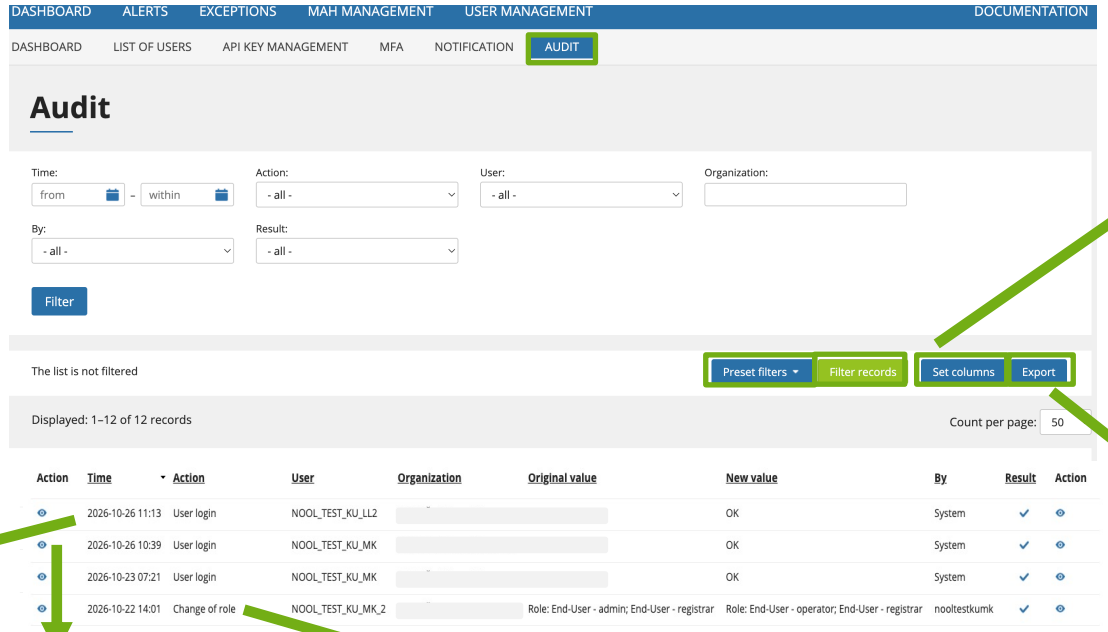


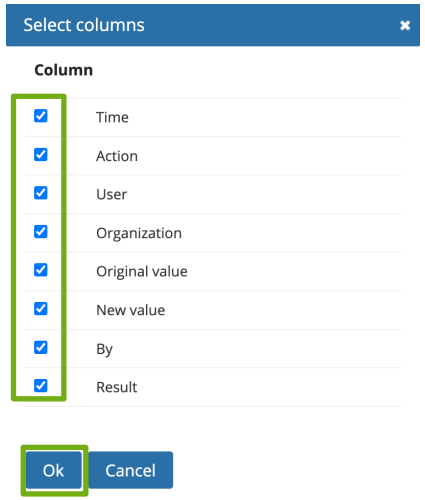
USER MANAGEMENT – AUDIT

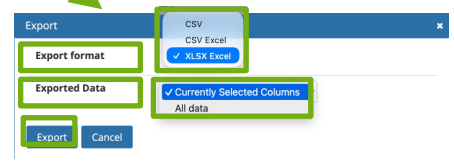
The "**AUDIT**" tab is a list of all important changes made to users (registration statuses, status changes, MFA changes, etc.).

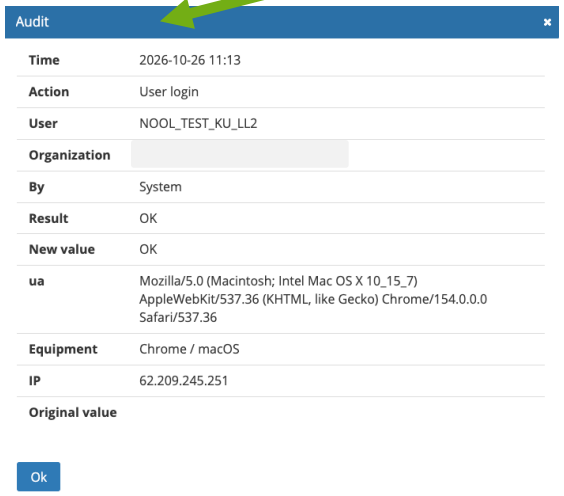
In the list, you can **set** the required **columns**, work with **filters** and **export** the data (CSV, Excel).

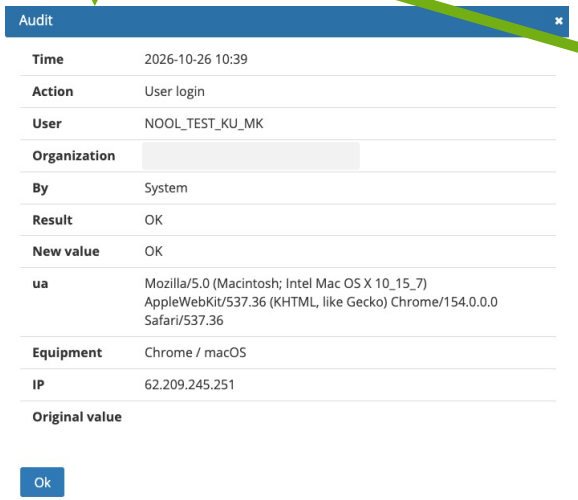
Clicking the "**eye**" icon next to a given user displays the detail of the logged event. See the examples below.

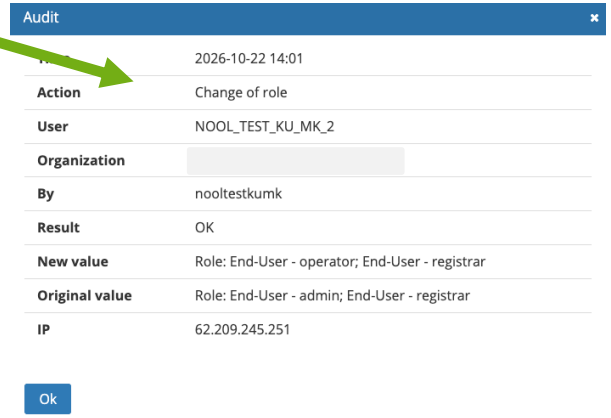












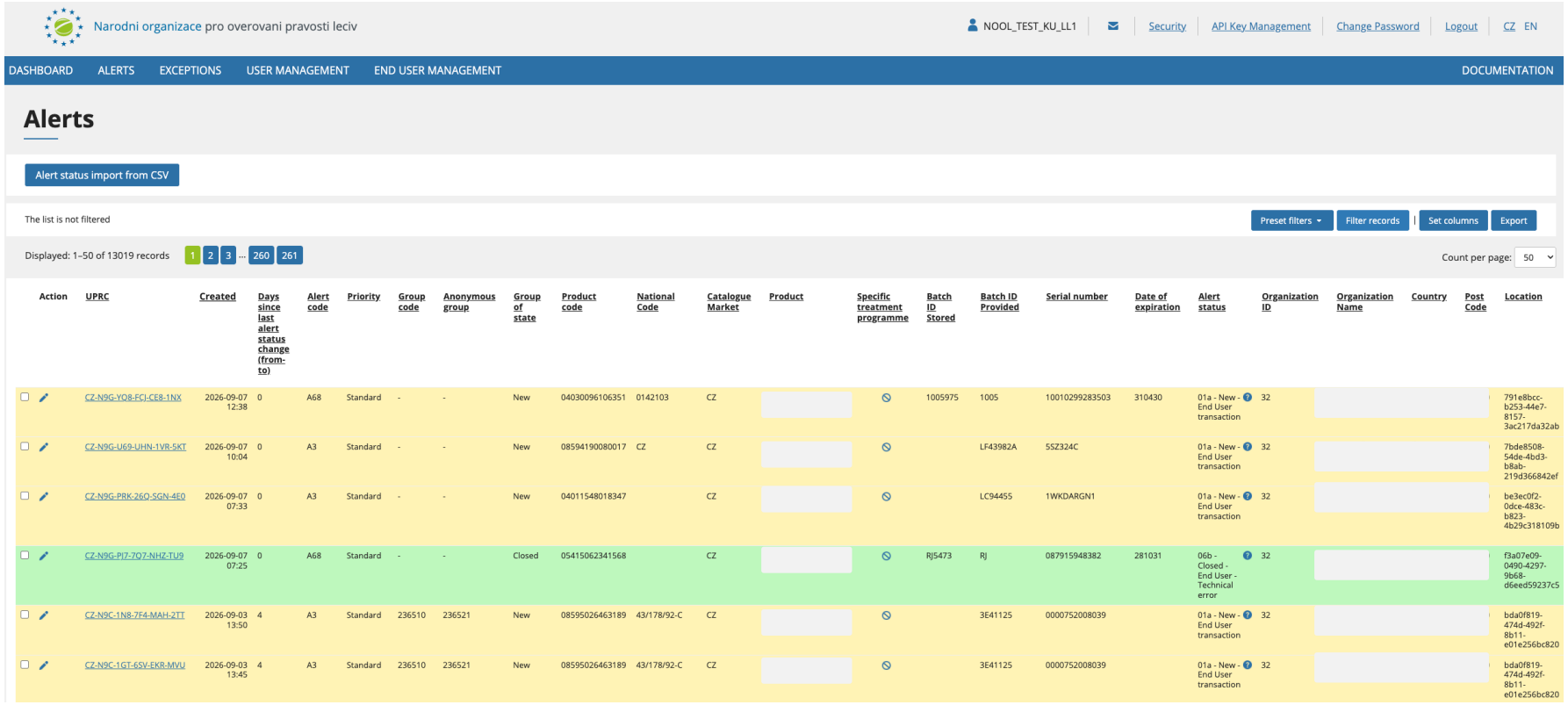
Part III

Alert Management

ALERT MANAGEMENT

The list contains all alerts belonging to the organisation and to the relevant user. This can be checked in User Management.

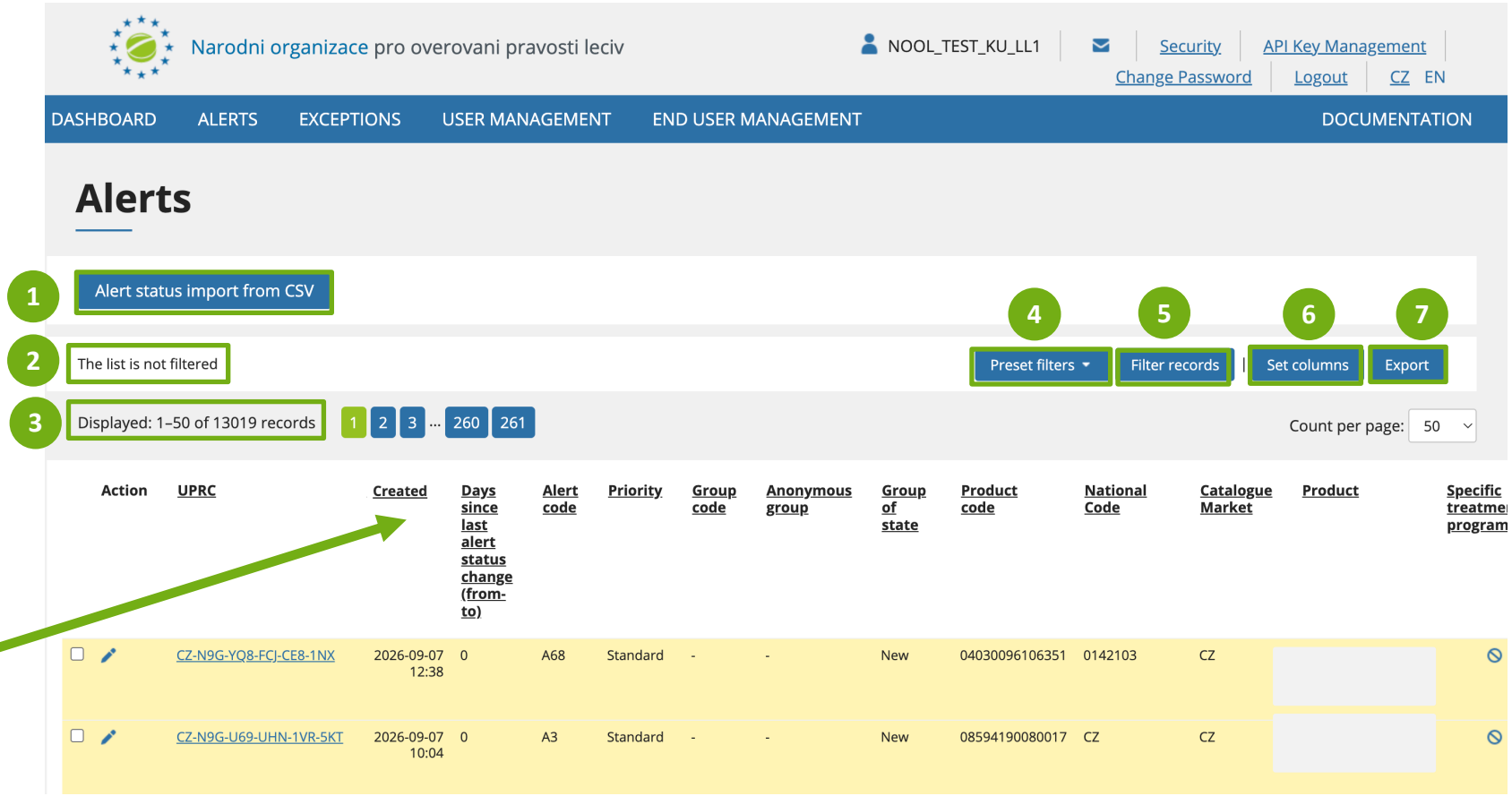
Note: The activities available to a user, and the resulting display of menus and options, depend on the user's role and permissions.



ALERTS - CONTROLS

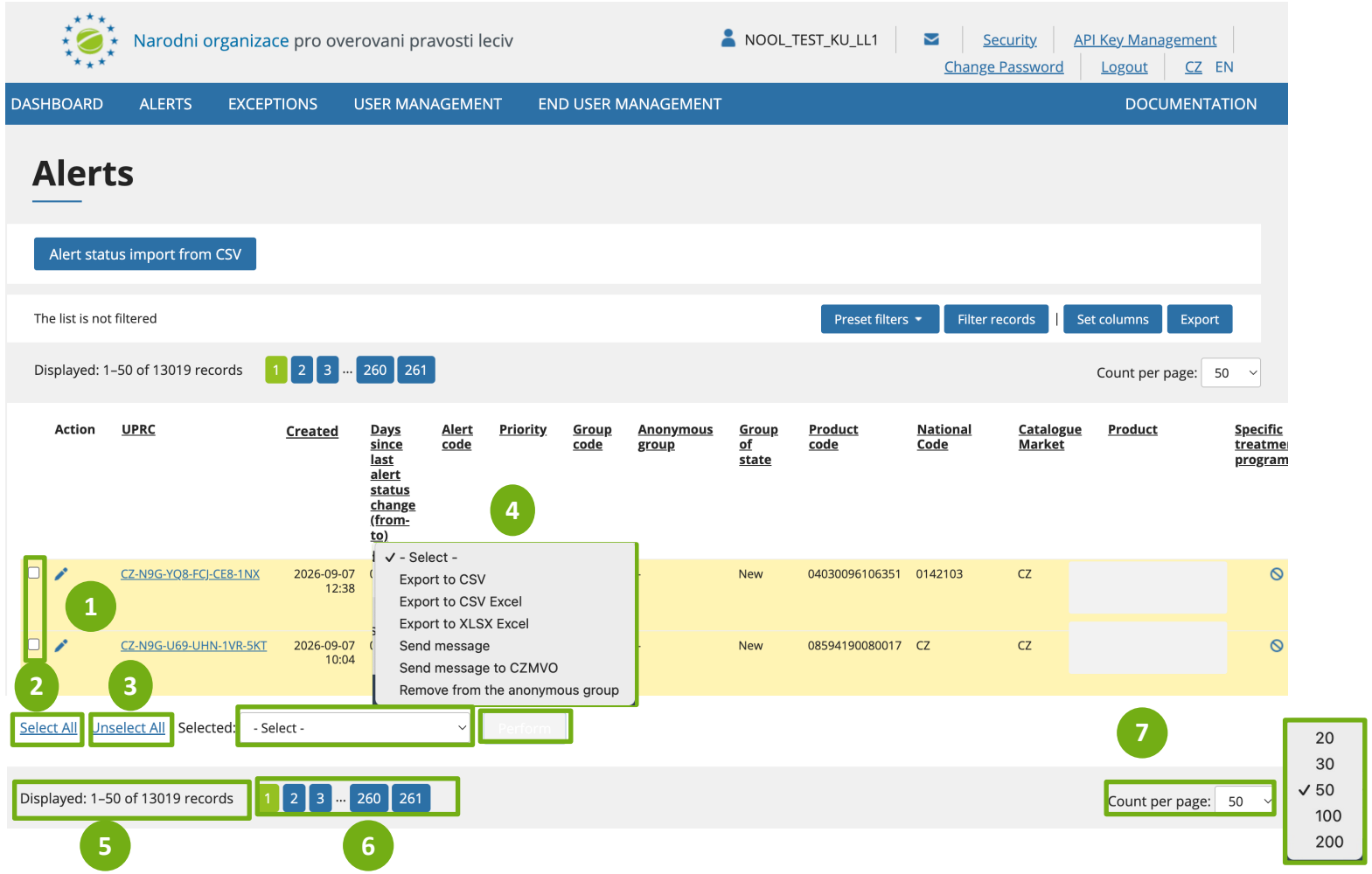
1. Bulk import of **alert-status changes** (emergency alert import).
2. Display of configured **filters**.
3. Display of the **number of alerts** matching the entered filter.
4. **Management of user filters.**
5. Show/hide the **filter**.
6. Configure the displayed **columns** in the alert list.

   Click a column header to sort items by that column.
7. **Export** — export alerts according to a preset, logs and a summary report for a selected period.



ALERTS - CONTROLS

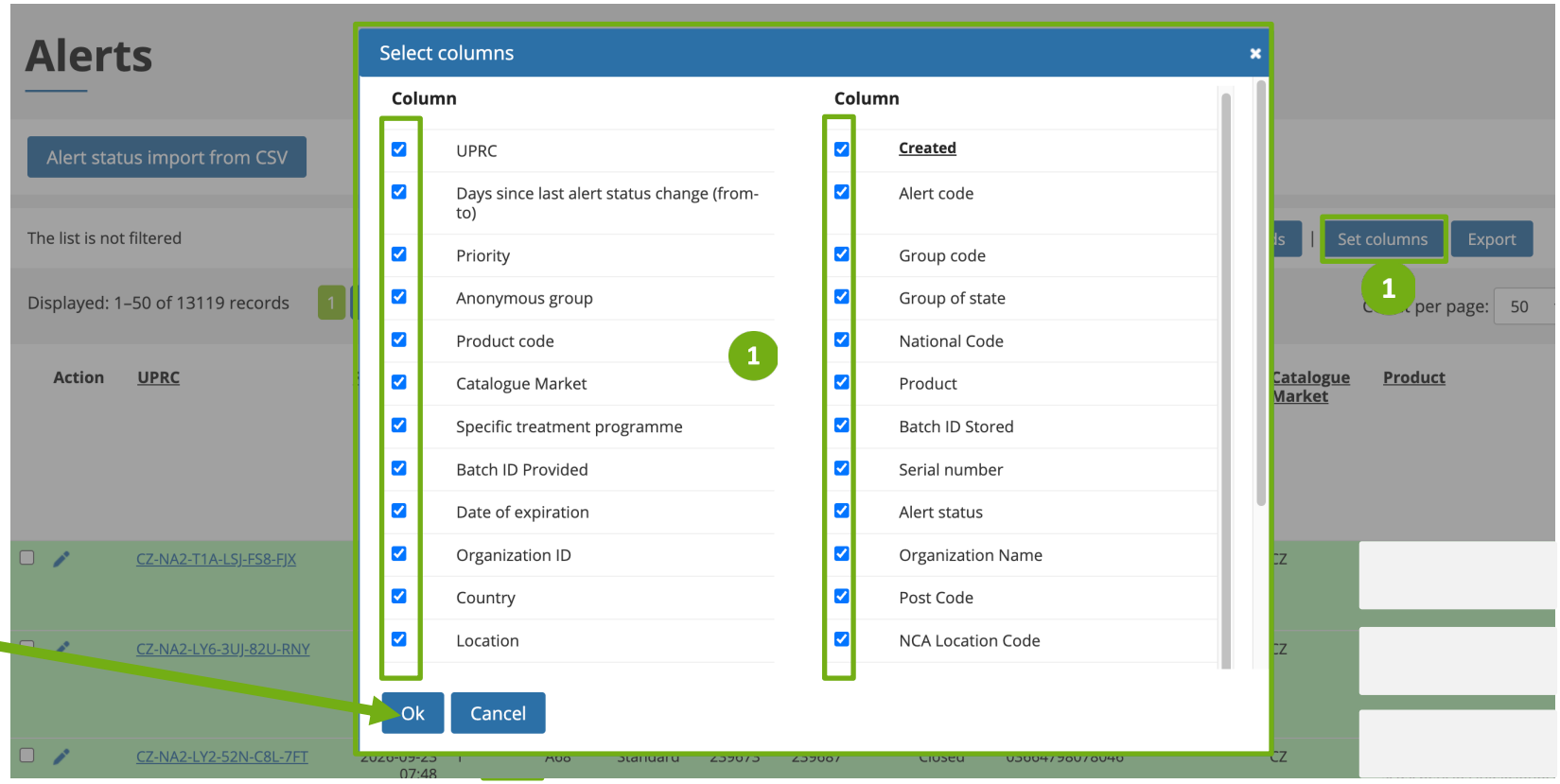
1. Click the checkbox to select an alert record; click again to clear the selection.
2. Select all items in the current selection/filter in bulk.
3. Clear the selection of items in bulk.
4. For selected items, you can perform **operations** from the menu: **Export** (CSV, XLSX), **Send message to MAH**, **Send message to CZMVO**, or **Remove items from anonymous group**.
5. Display the **number** of selected **records**.
6. Display the **number of pages** based on the selected number of records per page; use this for page navigation.
7. Choose the number of records displayed per page (range: 20–200).



ALERTS — CONFIGURING LIST OF COLUMNS

All columns are displayed by default.

The user can change the display by clicking „**Set columns**“. A window with a list of all columns opens. Select or clear checkboxes for the columns to show or hide, and confirm by clicking “**OK**“.



ALERTS - EXPORT

Click 1 „*Export*“

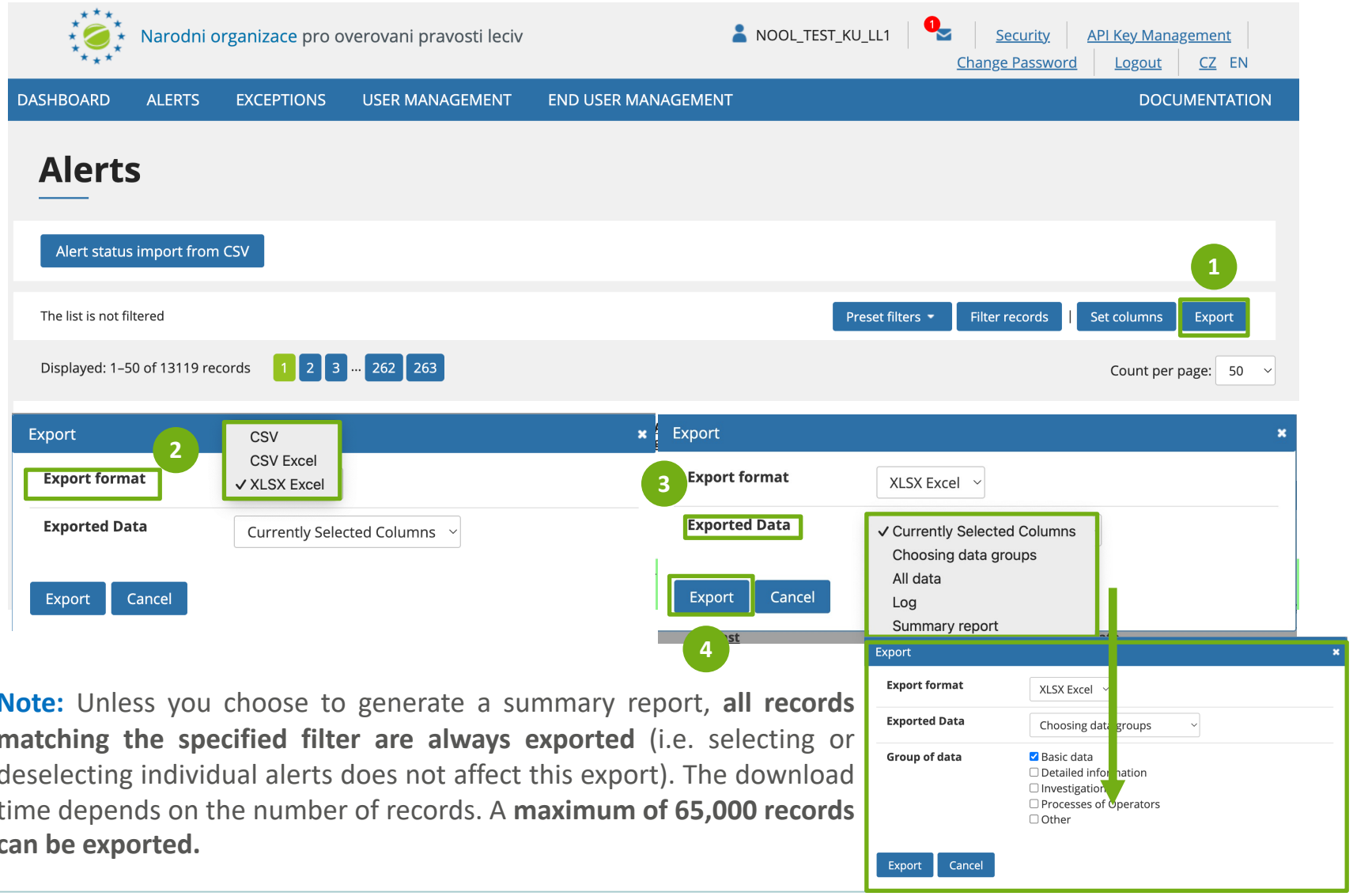
1. In 2 „**Export format**“, select the required output format: CSV, CSV Excel, XLSX.

2. In 3 „**Exported data**“, select the required export type.

You can export the **currently configured columns**, select data from **data groups**, or choose to export everything.

You can also export related **logging/audit records** or select the Summary report.

Click 4 „**Export**“. The file is saved to your default downloads folder.



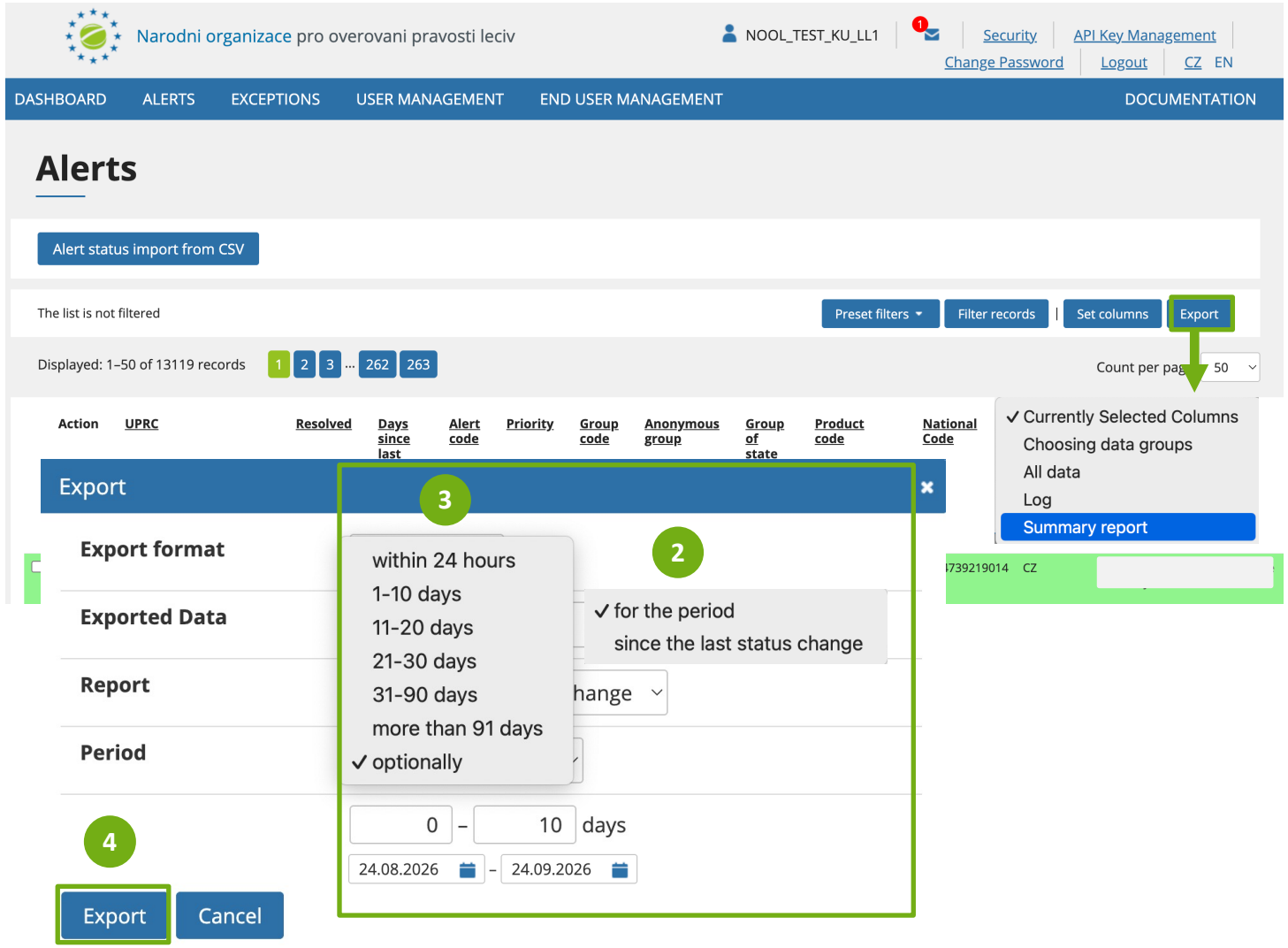
Note: Unless you choose to generate a summary report, **all records matching the specified filter are always exported** (i.e. selecting or deselecting individual alerts does not affect this export). The download time depends on the number of records. A **maximum of 65,000 records can be exported.**

ALERTS — SUMMARY EXPORT

„The Summary export“ 1 generates a summary overview of alerts for a specified period. The report can be generated for a 2 **specific period** or **since the last change was made**. Available formats are CSV, CSV Excel and XLSX Excel. You can choose a predefined period or enter a custom interval or dates. 3 Confirm report generation by clicking „Export“. 4

Example of a summary report for a selected period:

Report	for the period
Generated	2026-09-24 10:09
Period	2026-08-24 00:00-2026-09-24 23:59
Alert status	Number
01a - New - End User transaction	5
01c - Unknown MAH	1
03a - MAH/End User - unclosed alert older than 5 days	3
03b - MAH/End User - unclosed alert older than 10 days	1
06a - Closed - MAH error - Fixed	9
06b - Closed - End User - Technical error	70
06c - Closed - MAH error- Not fixed.	3
06d - Closed - MAH error - MH exception	40
06f - Closed - End User process error - cannot be dispensed	1
06m - Closed - End User process error – the pack can be supplied	1
Total	134
In the solution	10
Closed	124
From that mistake EndUser	0



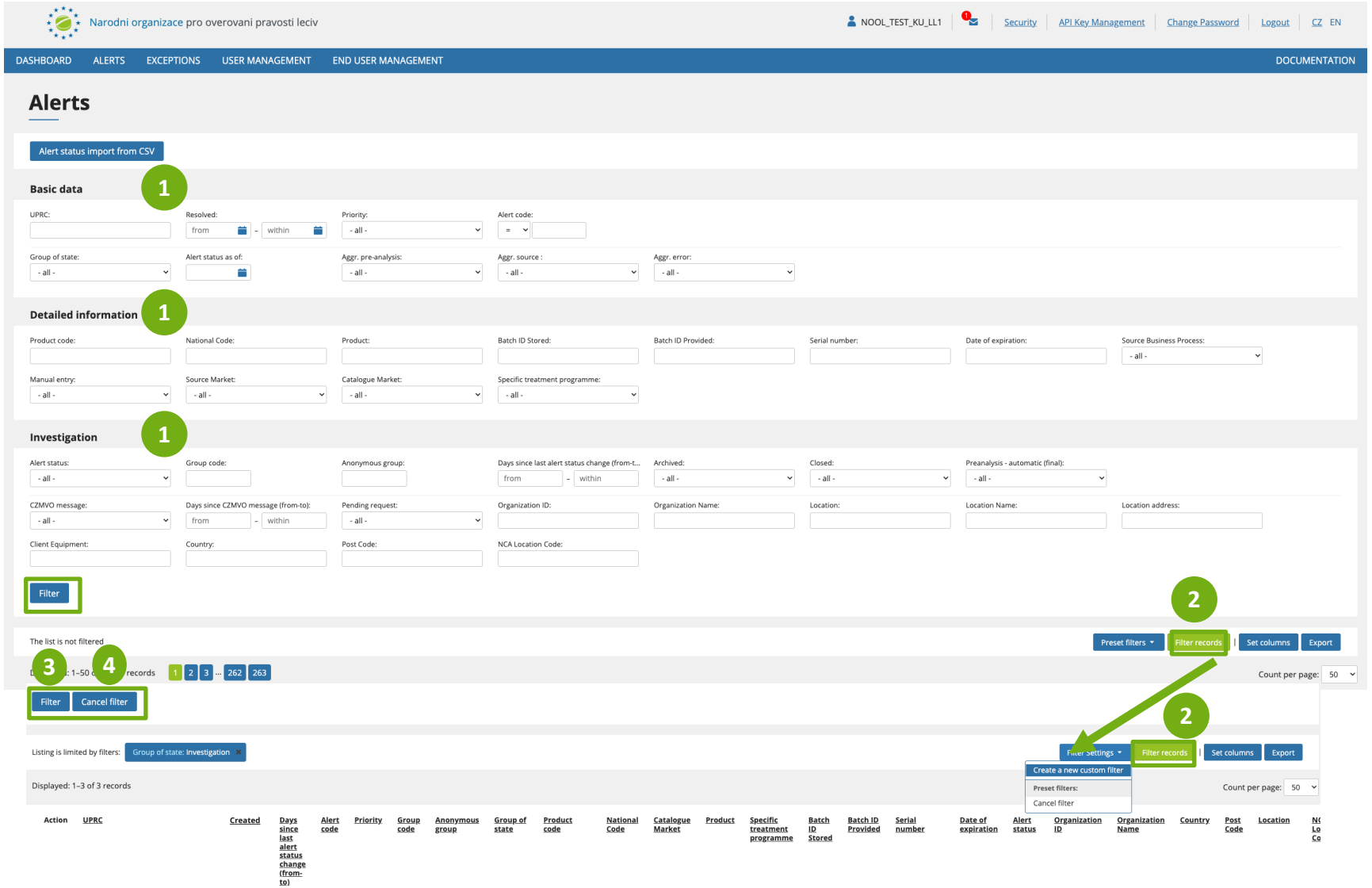
ALERTS - FILTERS

The alert list can be filtered by a number of criteria, including **UPRC, level, group number, batch, period, product code, serial number, alert error code, product name, status, multimarket, intermarket, business process** or **automatic pre-analysis** result, whether **additional information was requested**, and others.

For clarity, filters are grouped into three groups: „**Basic data**“, „**Detailed information**“ and „**Investigation**“. 1

Click „**Filter Records**“ to display the filter. Insert the required criteria and click „**Filter**“ or press „**Enter**“ 2 3

To cancel the filter click „***Cancel filter***“. 4



ALERTS - FILTERS

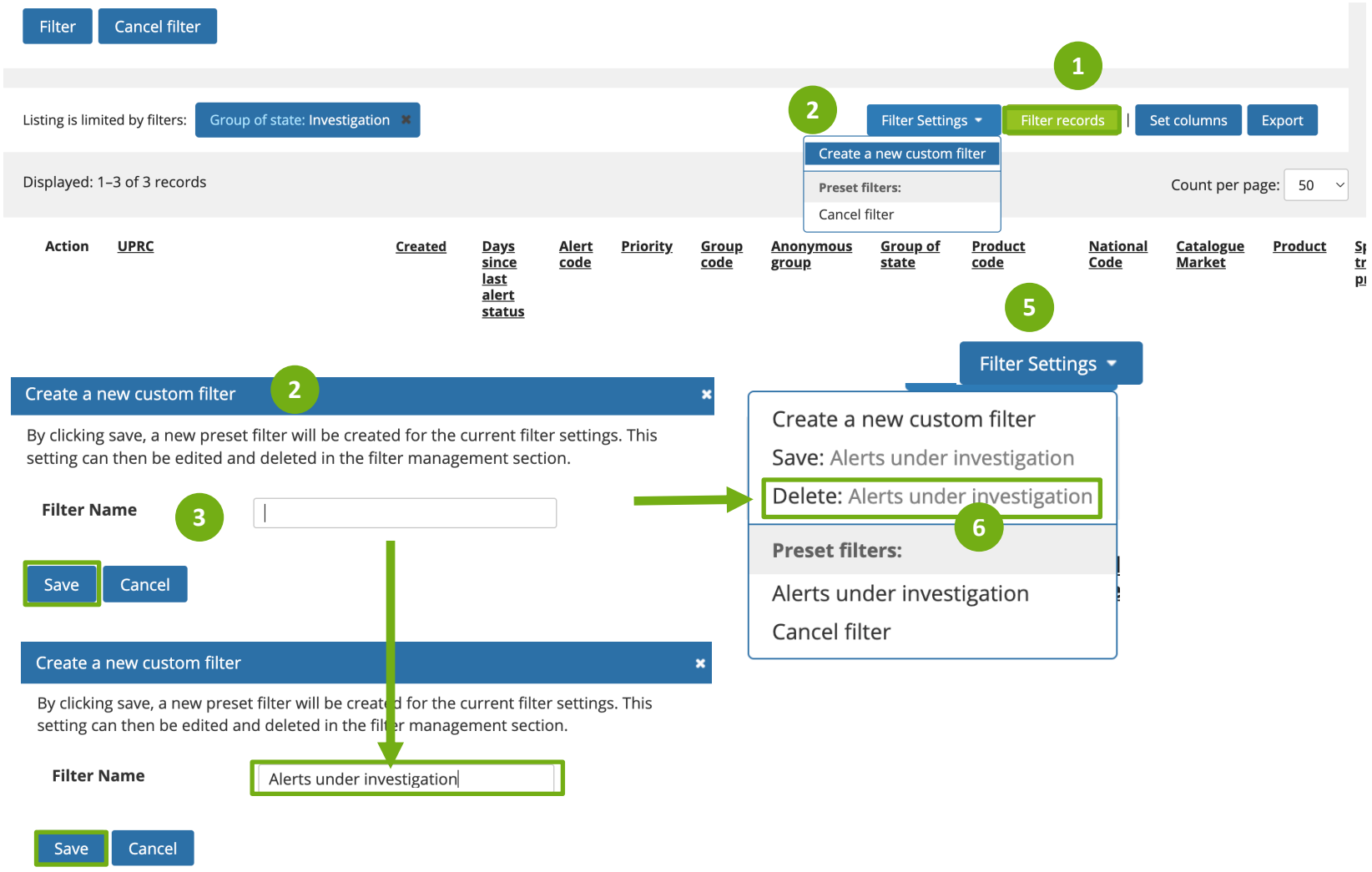
A user can create a **custom set of filters**, configure it, name it and save it. Clicking the required filter then displays the preset filter and generates the required selection of records.

Click „**Filter records**“ to display the filter. 1

Enter the required criteria and click „**Create a new custom filter**“. 2

Enter the „**Filter name**“ and save it to the filter list by clicking Save. 3 4

Under „**Filter settings**“, activate or delete the required filter by choosing **Delete**: “filter name”. 5 6



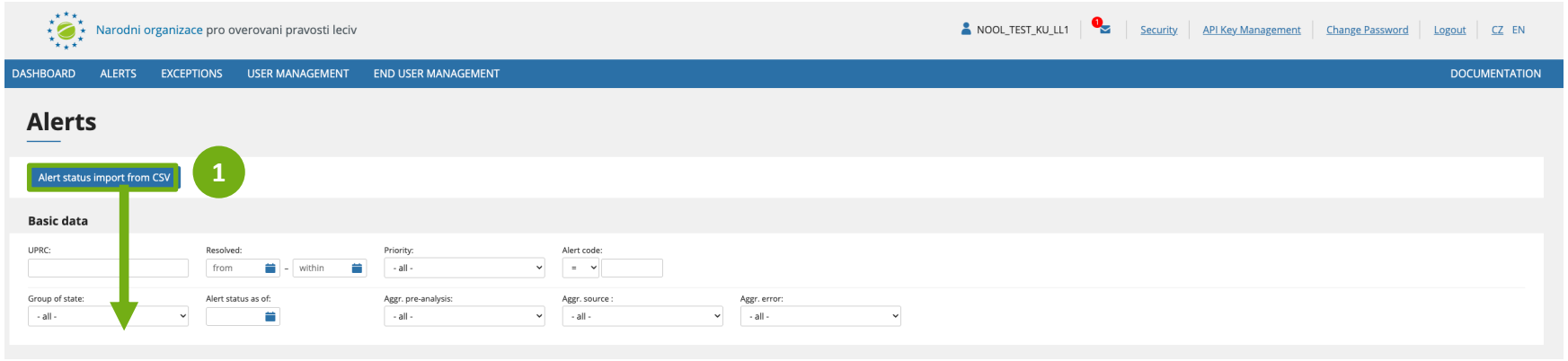
ALERTS — BULK ALERT STATUS CHANGE

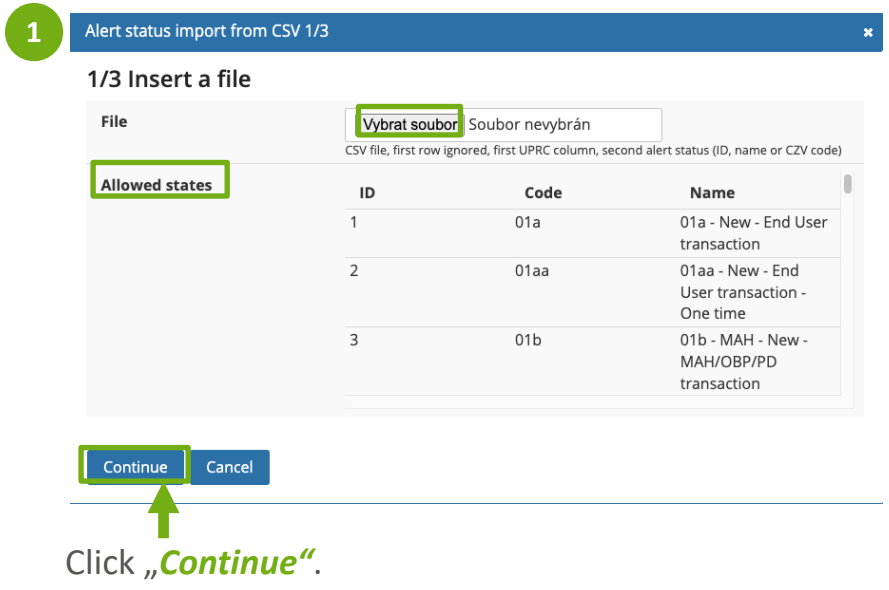
To change **alert statuses in bulk**, you can import a CSV file into CZAMS containing a list of alerts and the ID of the status you want to assign to them. The requested status change must comply with the process workflow; otherwise, the system will not perform the change.

In Record filter, click "***Alert status import from CSV***".

Then select and upload the prepared CSV file.

Note: The "**Allowed states**" table lists all status IDs, codes and names. Each row in the CSV file must contain the alert's "**UPRC**" and the "**Alert status ID**" you want to assign. These two values must be separated by a **comma**.



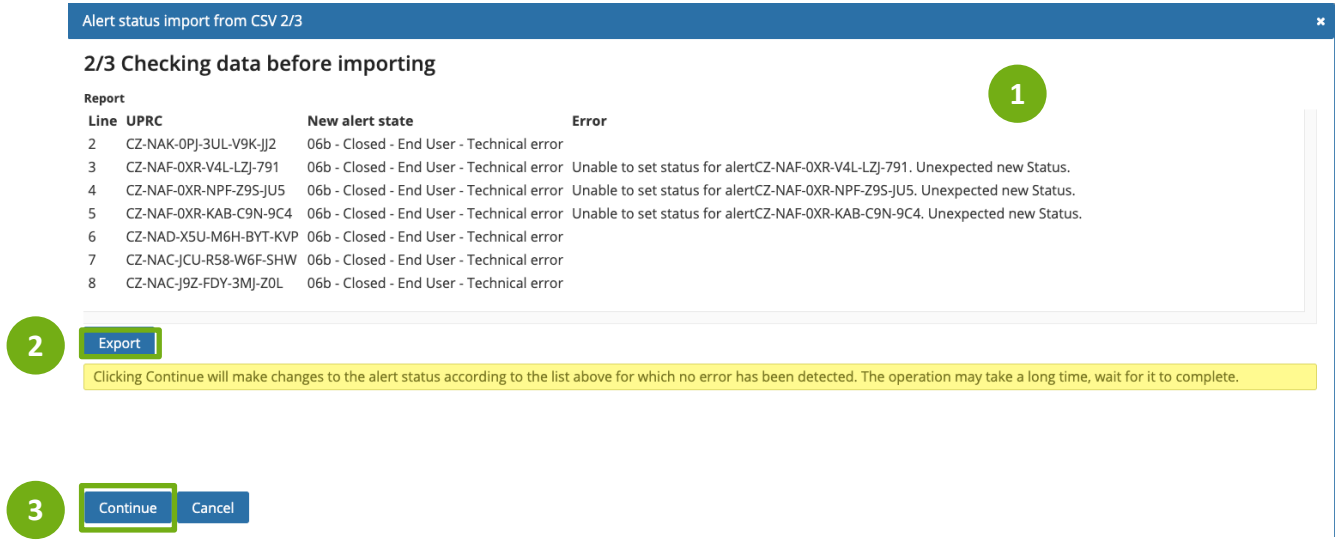


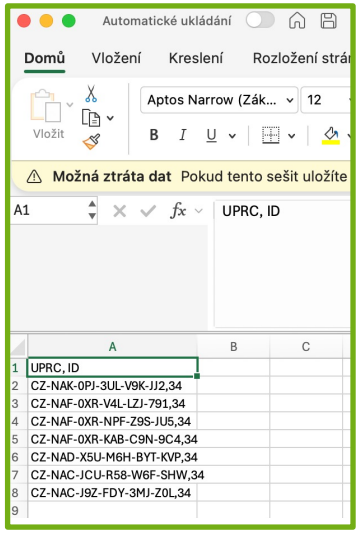
Click „***Continue***".

ALERTS — BULK ALERT STATUS CHANGE

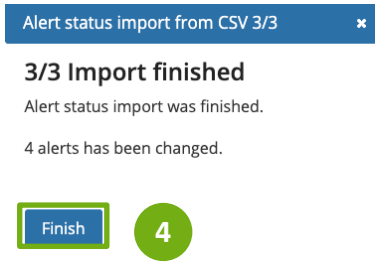
Example:
In the example below, we want to assign the status "*06b - Closed - End User - Technical error*" to the listed alerts. This status has ID 34.

The first row in column A may contain any values; the system will ignore it. The **UPRC** and **alert status ID** values must therefore start **in the second row of column A**. **All other columns must remain empty**; otherwise, the system will consider the file invalid.





1. If the file is correctly formatted, a list of the alerts whose statuses are to be changed is displayed. The status to be assigned is shown in the "*New alert status*" column.
2. Click "Export" to generate an "**Import report**".
3. After checking the data, click "***Continue***"

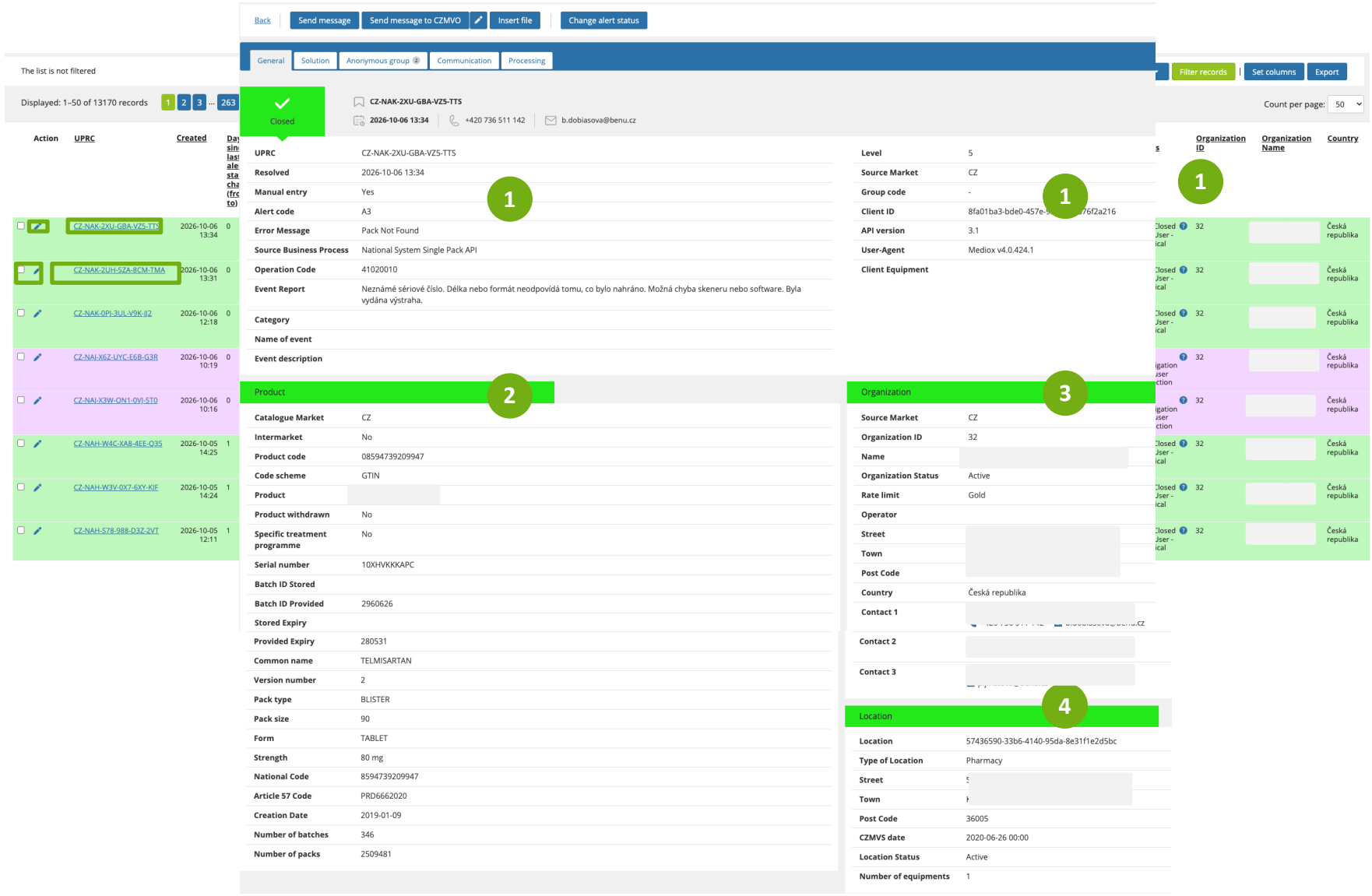


If the requested status change complies with the process workflow, the alert statuses are changed as requested. Click "***Finish***". 4

ALERTS – ALERT DETAILS

Click the alert „UPRC“ or the „pencil „icon. A page containing all available detailed information about the selected alert opens.

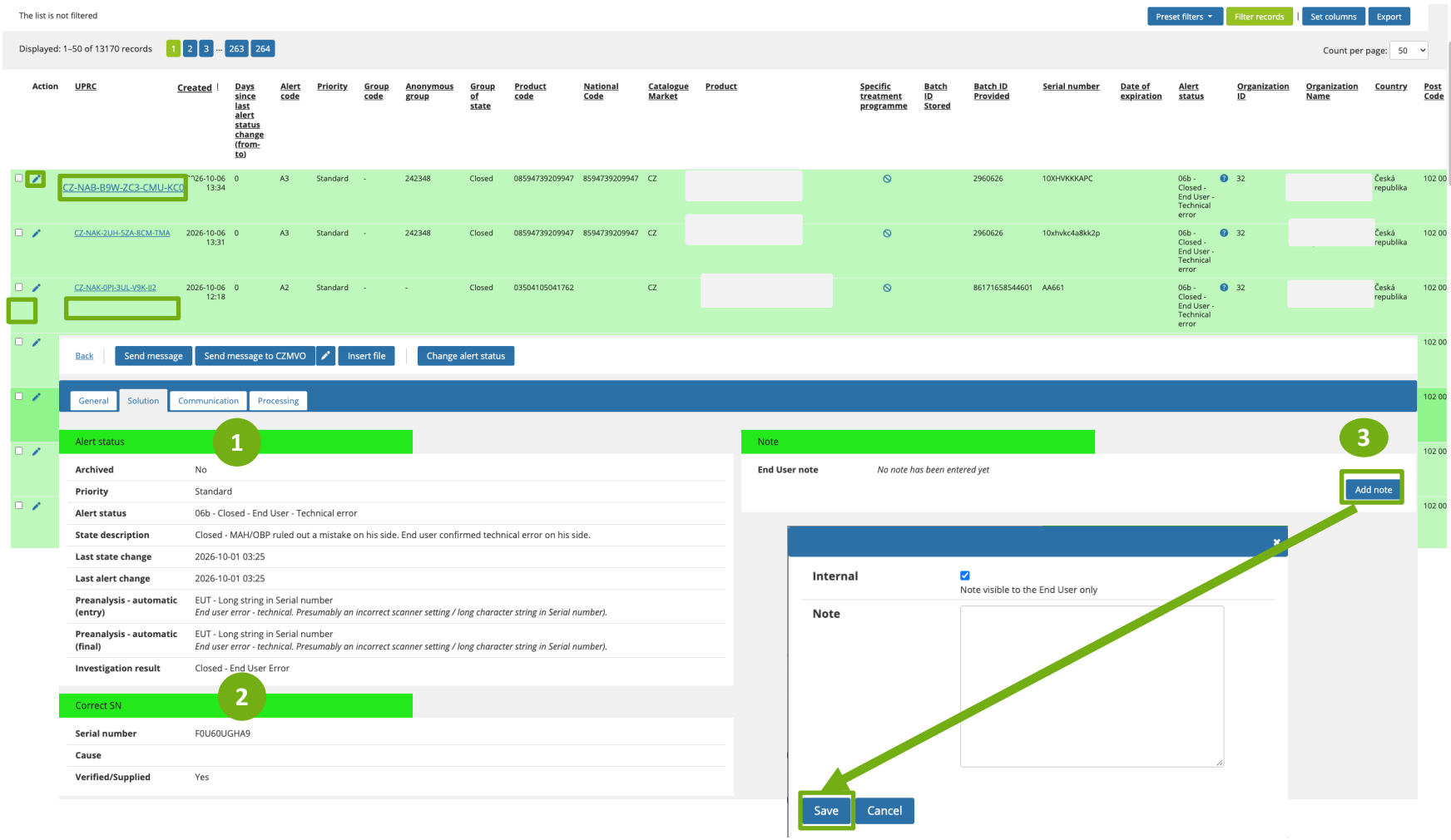
- The page may contain four to seven tabs, depending on the alert type and the stage of the investigation.
- The „General“ tab is divided into four sections: 1
- All currently available information about the alert, including UPRC, date and time of creation (UTC), alert code, operation code, transaction type, group code if assigned, API version used and software version. All available product information, 2 including batch, serial number, expiry date, pack, the number of batches and packs planned for supply to the Czech market, the SIDC code where known, and other details. Information about the Organisation. Location at which the alert was generated. 3 4



ALERTS – ALERT DETAILS – SOLUTION

The „**Solution**“ tab, in the (1) **Alert status** section, contains basic information about the status of the selected alert, for example priority, alert status, and the date and time of the last status change. It also displays the automatic pre-analysis results, both initial and final, and the final investigation outcome. For some technical alerts, a (2) „**Correct SN**“ section may be displayed. It contains the result of an analysis of the serial-number format provided by MAH/OBP in the product catalogue, compared with the serial number entered into CZMVS. The „*Cause*“ field also describes the difference found between the correct serial number and the serial number entered into CZMVS.

The (3) „**Note**“ section allows you to click „**Add note**“. A note may be internal, visible only to the relevant end user, or visible to other users with the appropriate role and permissions.



ALERTS – CREATING AND VIEWING ALERT GROUPS

Grouping alerts

- ✓ Creating groups is an automatic system function for grouping alerts that are likely to have the same cause within a specified time interval. The default interval is one day; the user can change it.

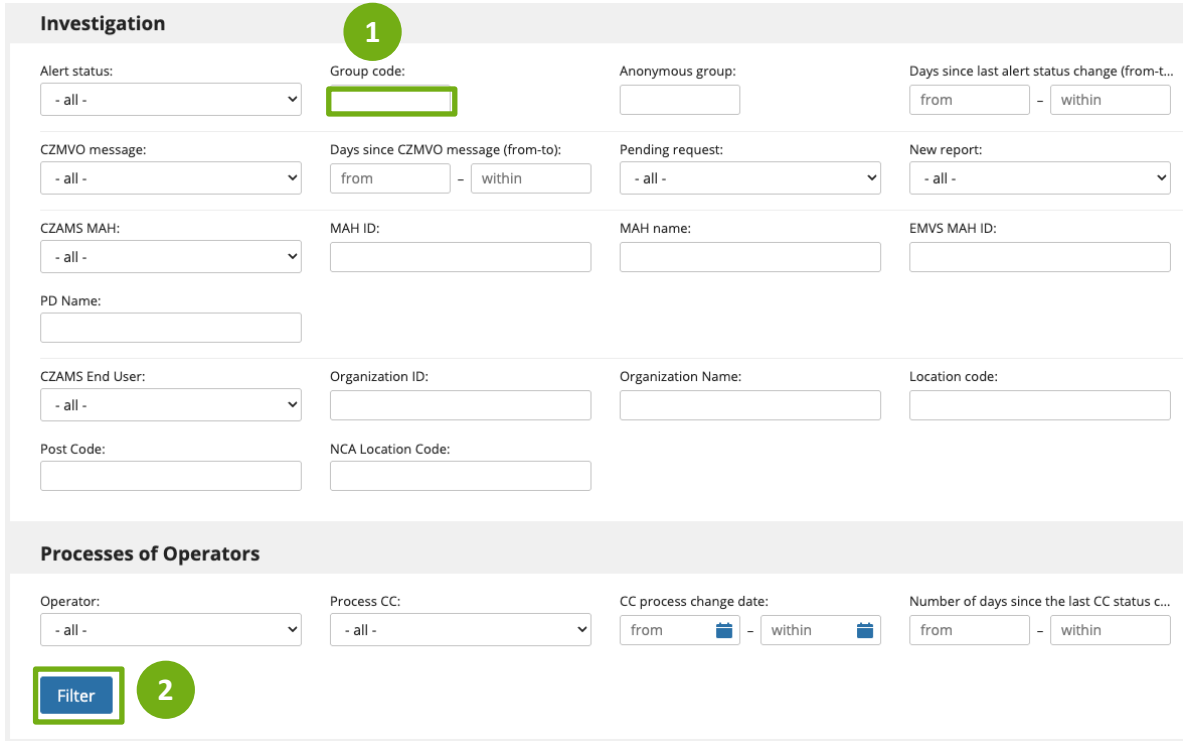
The system creates **two types of groups**:

GROUP

- ✓ Grouping is based on **MAH, product code, error code, batch and, where applicable, expiry date.**
- ✓ A group always consists of products with **the same product code**.

ANONYMOUS GROUP

- ✓ Grouping is based on **the error code** and **location**.
- ✓ A group is always **created within one location**.
- ✓ This group is not displayed to MAH/OBP. It is intended only for the end user (pharmacy or wholesaler).



1 To display a group or anonymous group, use a filter. Enter the group number in the „**Group code**“ field and click „**Filter**“.2

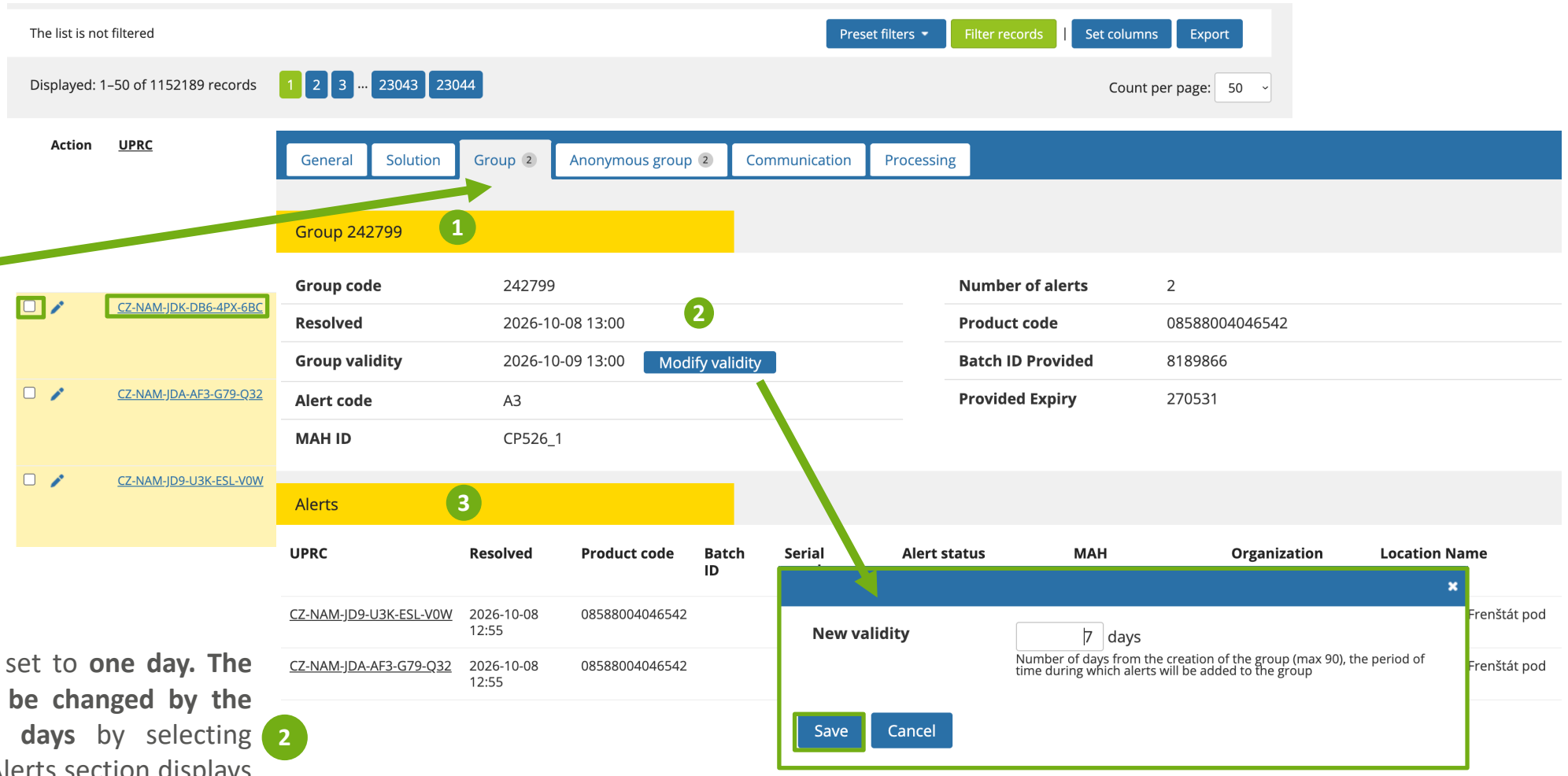
If you do not know the group or anonymous-group number, you can find it in the alert list. Find an alert belonging to the group; the group number is displayed in the Group code column. An alert for which no group number is displayed is standalone and does not belong to any group.

ALERTS – ALERT DETAILS – GROUP

The „**Group**“ tab displays information about the alert group to which the alert was assigned automatically. The number of alerts in the group is indicated by a number.

The 1 section displays basic group information: group code, creation date, period for which the group will be formed (validity), alert code, product code, batch, expiry date...

By default, validity is set to **one day. The number of days can be changed by the user from 1 to 90 days** by selecting **Modify validity**. The Alerts section displays basic information about all alerts in the anonymous group. 3



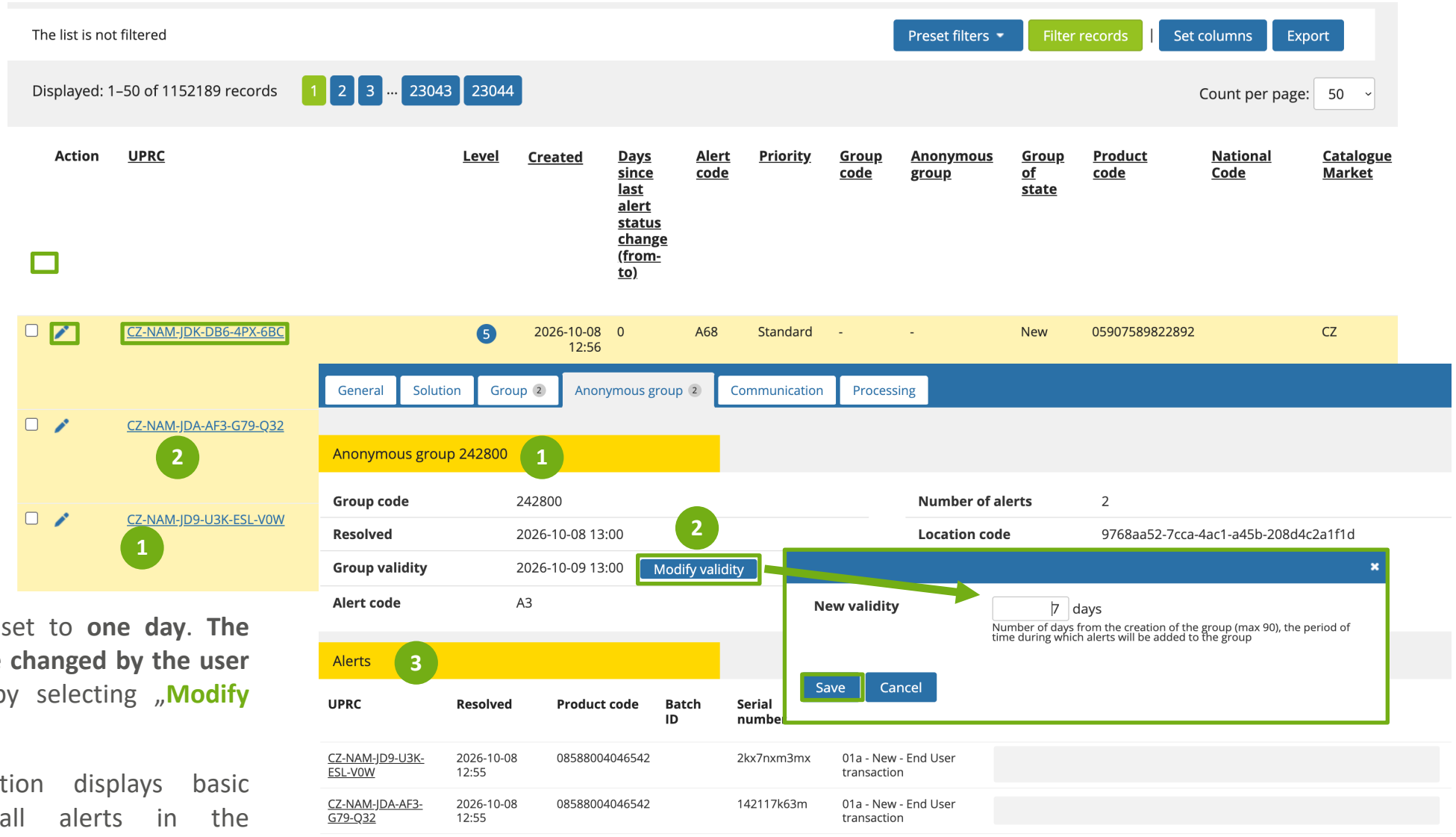
ALERTS – ALERT DETAILS – ANONYMOUS GROUP

The „**Anonymous group**“ tab displays information about the anonymous alert group to which the alert was assigned automatically.

The section 1 displays basic anonymous-group data: group code, creation date, the period for which the group is formed (validity), alert code, number of alerts in the group and location ID.

By default, validity is set to **one day**. **The number of days can be changed by the user from 1 to 90 days** by selecting „**Modify validity**“. 2

The 3 Alerts section displays basic information about all alerts in the anonymous group.

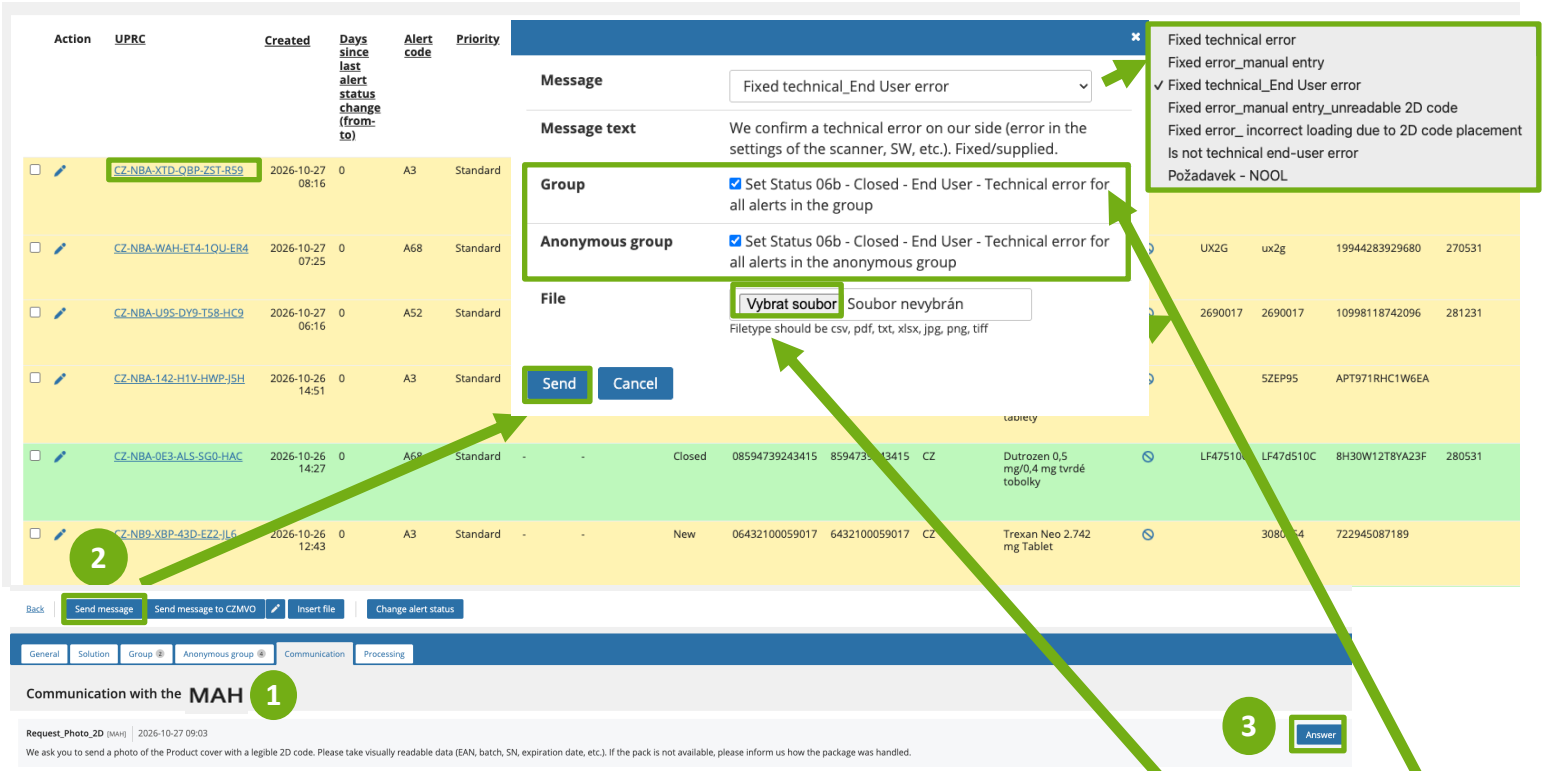


ALERTS - ANONYMOUS COMMUNICATION WITH MAH/OBP

The Alert Management System supports the **anonymous exchange of predefined bilingual messages (English/Czech)** between the end user and MAH/OBP. This communication supports and facilitates the investigation process.

For example, end users can use this feature to inform MAH/OBP when they discover that an error occurred on their side, or to respond to an MAH/OBP request. They send the message in Czech, and MAH/OBP sees it in English.

The communication overview is available under the "**Communication**" 1 tab in the alert detail.



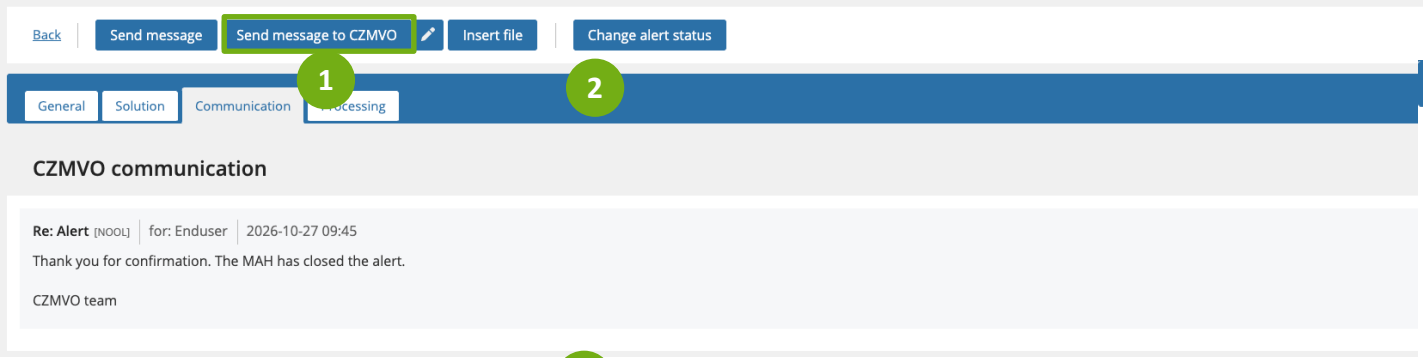
To send a message to the end user, click 2 "**Send message**". A dialog window opens. Select the required predefined message from the "**Message**" drop-down menu. The available messages correspond to the alert's specific status and type. They are continuously updated and supplemented according to user requirements. Select "**Group**" to send the message to all alerts in the group. The same applies to "**Anonymous group**".Use "**Select file**" to attach a file. Click "**Send**" to send the message. You can also respond to a received message using 3 "**Reply**". The available messages are the same as under "**Send message**", but a reply cannot be sent to multiple alerts in a group.

ALERTS – COMMUNICATION BETWEEN USER AND CZMVO

Warning:

Unless the cause of the alert is clearly attributable to the end user (e.g. a technical scanning error, a process error, etc.), MAH/OBP is always responsible for investigating and correctly closing the alert. **MAH/OBP automatically receives a notification after 5 days**, followed by a further warning about the unresolved alert after **another 5 days**. If MAH/OBP **still has not responded 30 days after the alert was generated, SIDC is informed of its inactivity.**

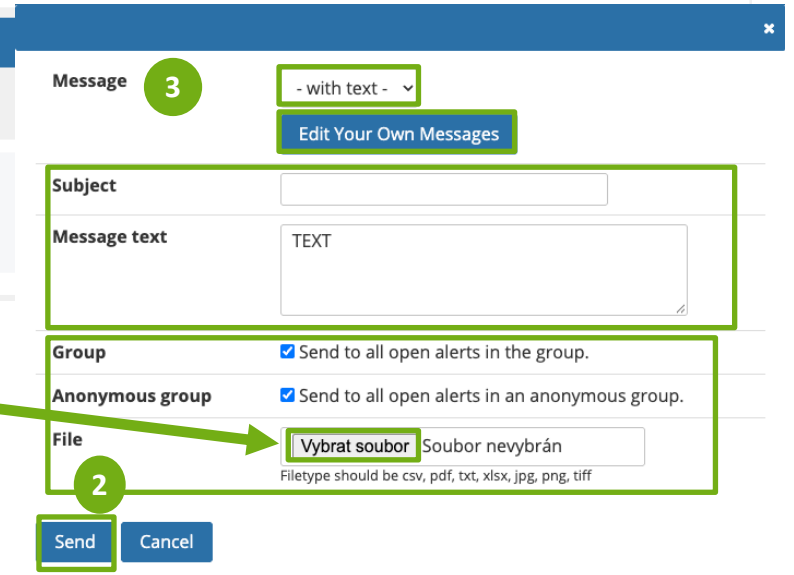
If MAH is inactive, or for other reasons, the end user can communicate directly with CZMVO using "Messenger CZMVO".



To send a message to CZMVO, click 1 "***Send messge to CZMVO***". A dialog window opens in which you can enter the **message subject and any text**. Use "***Select file***" to attach a file if required. Click 2 "***Send***" to send the message to CZMVO. Messages can also be sent to all open alerts in a Group or Anonymous group.

Note: The text may be in any language; however, **Czech** or **English** makes CZMVO's work easier.

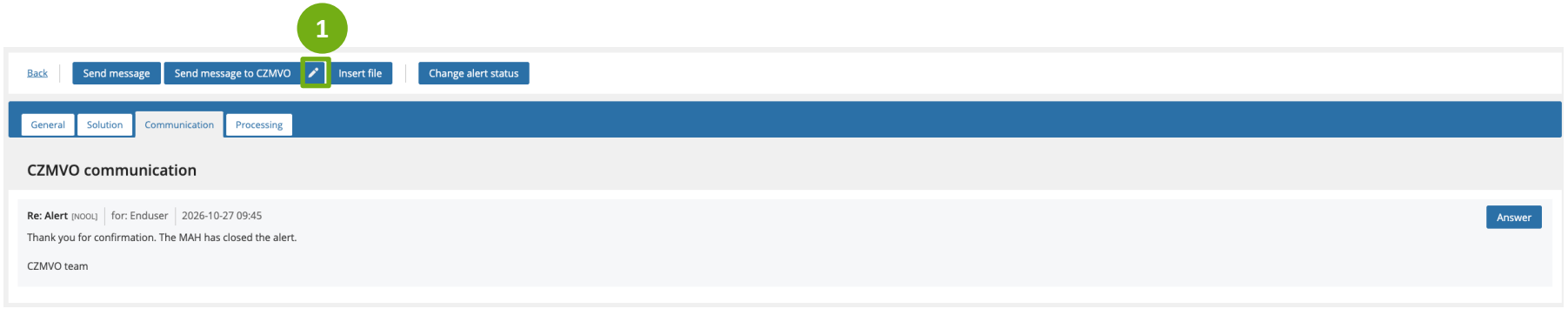
This communication supports and facilitates the alert investigation process and **does not affect the alert status.**



Under 3 Message", you can enter a text message or, if available, select one of your own message templates and edit it as needed before sending

ALERTS – COMMUNICATION BETWEEN USER AND CZMVO

User can create a **set of templates for the messages they most frequently exchange with CZMVO**.



To create, edit or delete user message templates for CZMVO, click the 1 **„pencil icon“**. In the message list, click “**Add custom message”.** 2

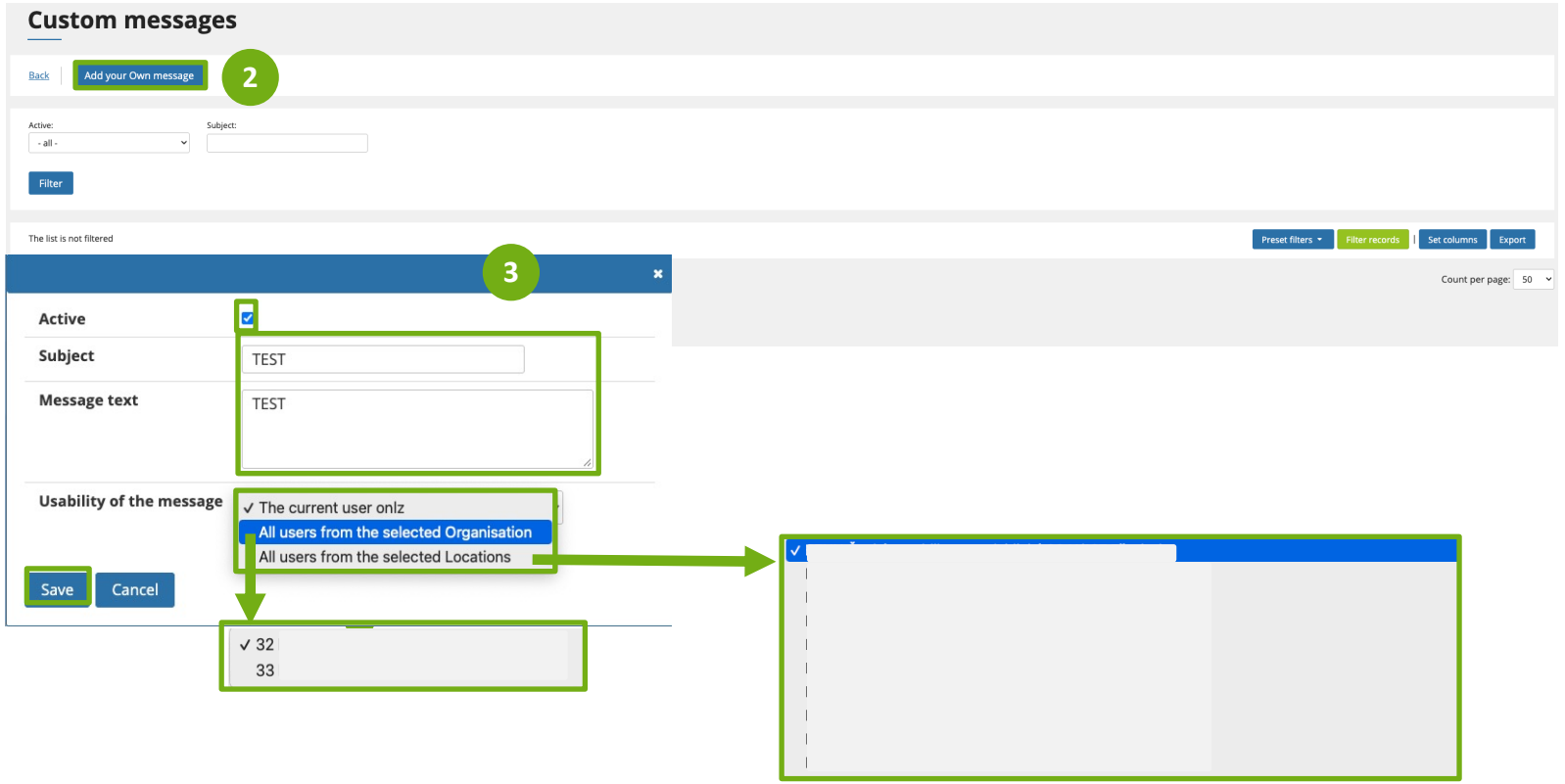
In the dialog 3 window, specify whether the message should be **active**, enter the **message subject and add the message text**. From the “**Usability of the message**” menu, select one of the following **three options**:

a) **Current user only** — if the message will only be used by the person creating it.

b) **All users in the selected Organisation.**

c) **All users at the selected Location.**

Click “**Save**” to save the message.



ALERTS – COMMUNICATION BETWEEN USER AND CZMVO

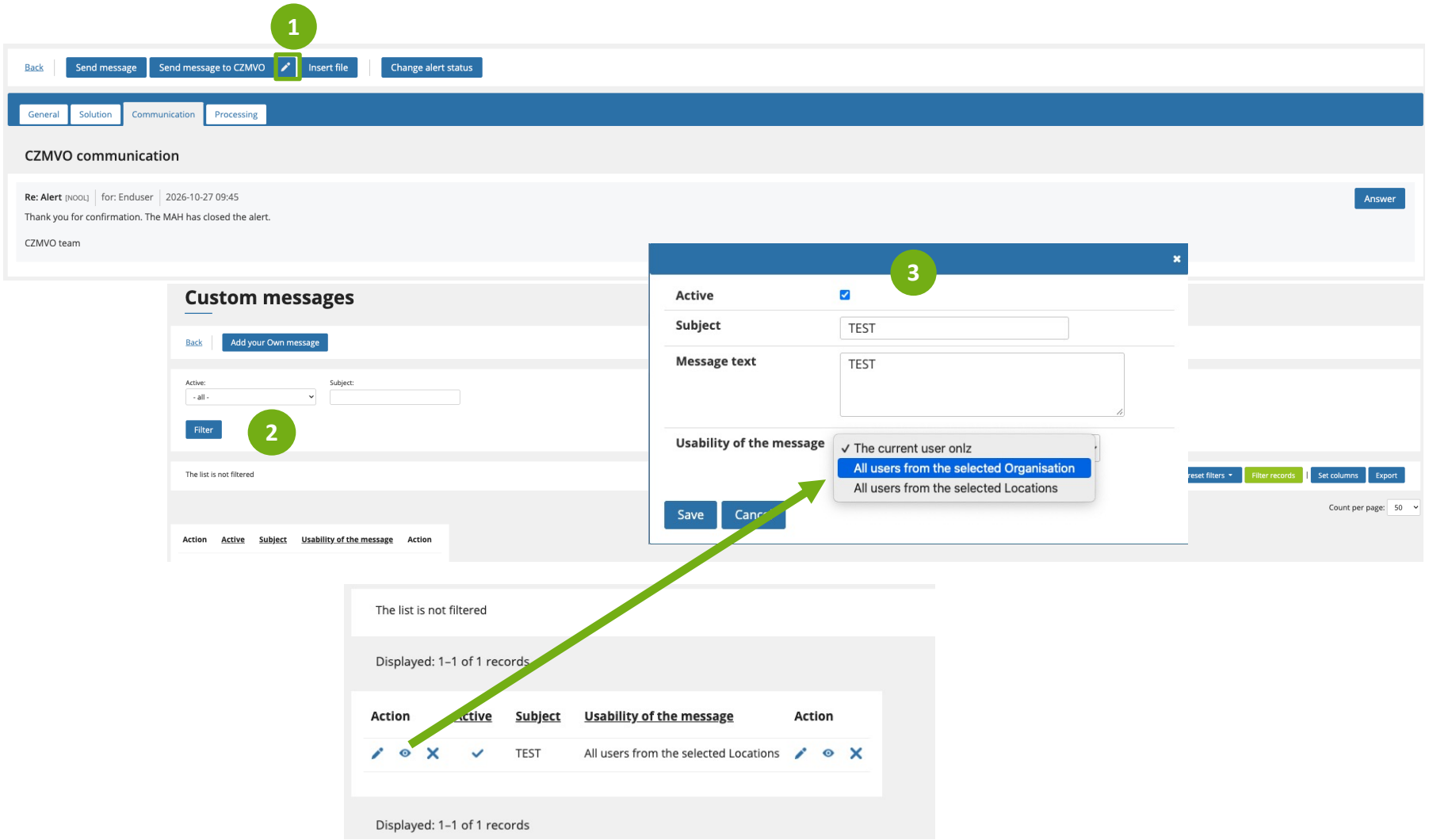
Users can manage their message **templates by editing, adding or deleting them.**

Click the „**pencil icon**“ (1) to open the list of preset user messages.

Use the filter (2) to search for messages.

Click the „**eye icon**“ to display the message details. (3)

Click the „**pencil icon**“ to edit a message, or click “**x**” to delete it.



ALERTS — COMMUNICATION — LIST OF ALERTS WITH A REQUEST FOR ADDITIONAL INFORMATION

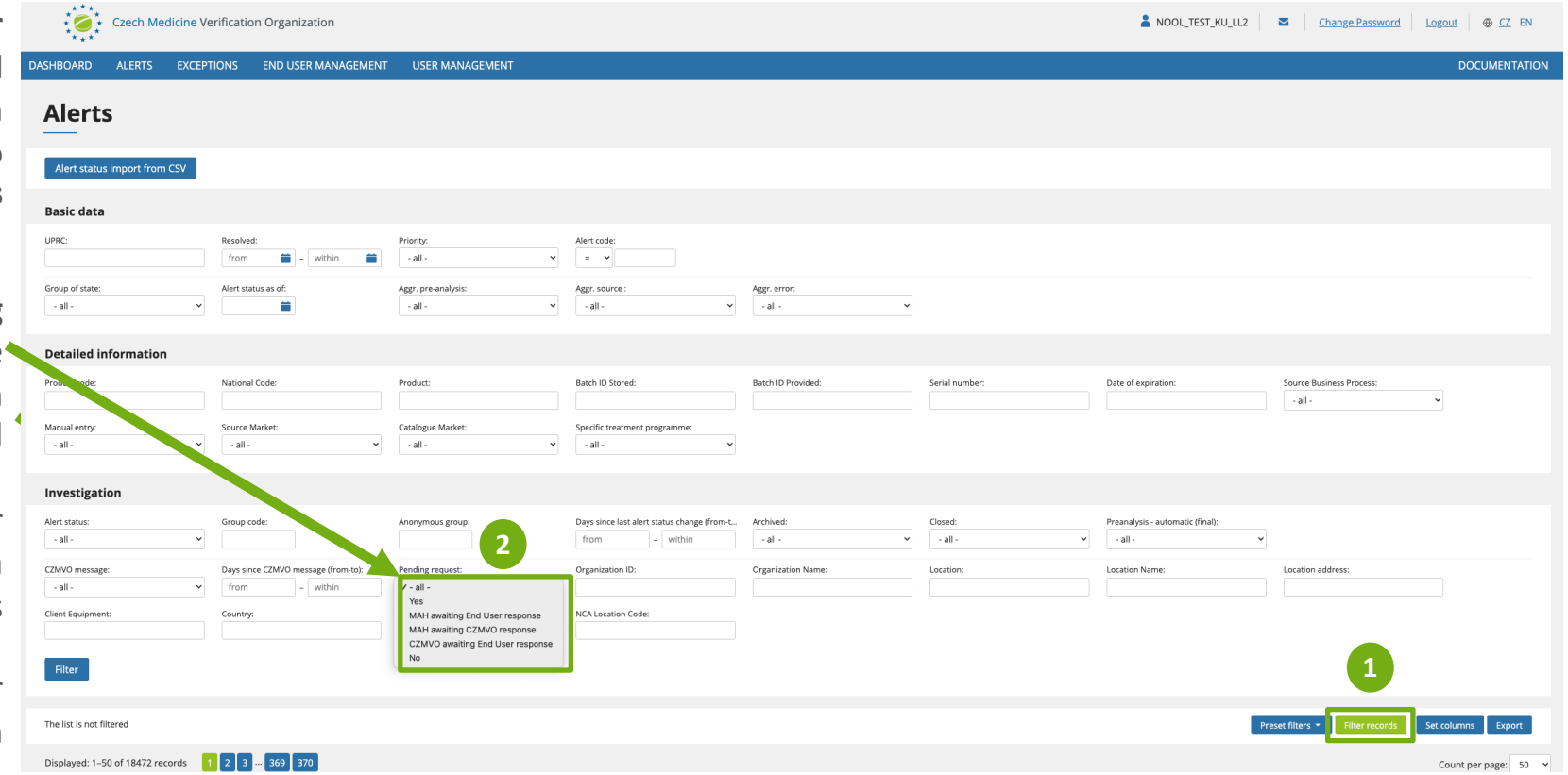
The easiest way to view the list of alerts for which MAH/OBP has requested additional information is through the Dashboard, which includes an option specifically designed to help users **quickly find outstanding requests** (see the section 11 Dashboard).

You can also obtain this information using filters. Click 1 "**Filter Records**" to display the filter. In the 2 "**Pending request**" drop-down menu, select one of the options below and click "**Filter**" or press „**Enter**".

"**MAH from End user**" — MAH's request for information from the end user (e.g. a photograph of the pack). The alert is in status "**04a**", "**03c**" or "**03d**".

"**MAH from CZMVO**" — MAH's request for information from CZMVO. The alert is in status "**04b**".

"**CZMVO from End user**" — CZMVO's request for information from the end user. The alert is in status "04d"

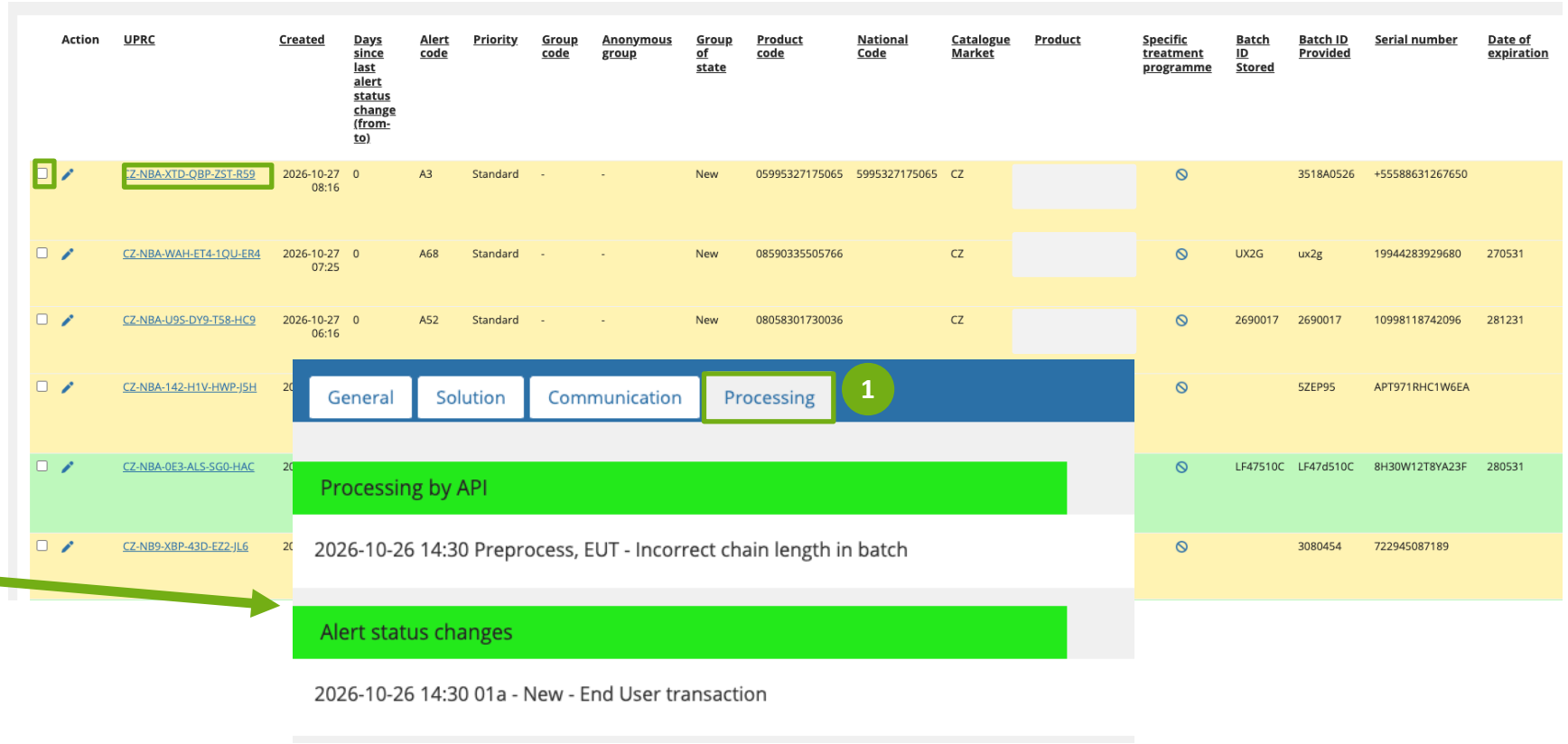


ALERTS – ALERT DETAILS - PROCESSING

The Alert Management System **records all important activities associated with alert investigations in system logs**. These include all status changes, recording when each change was made, who made it and what was changed.

Users can view some of these records by clicking the "**Processing**" tab in the alert detail.

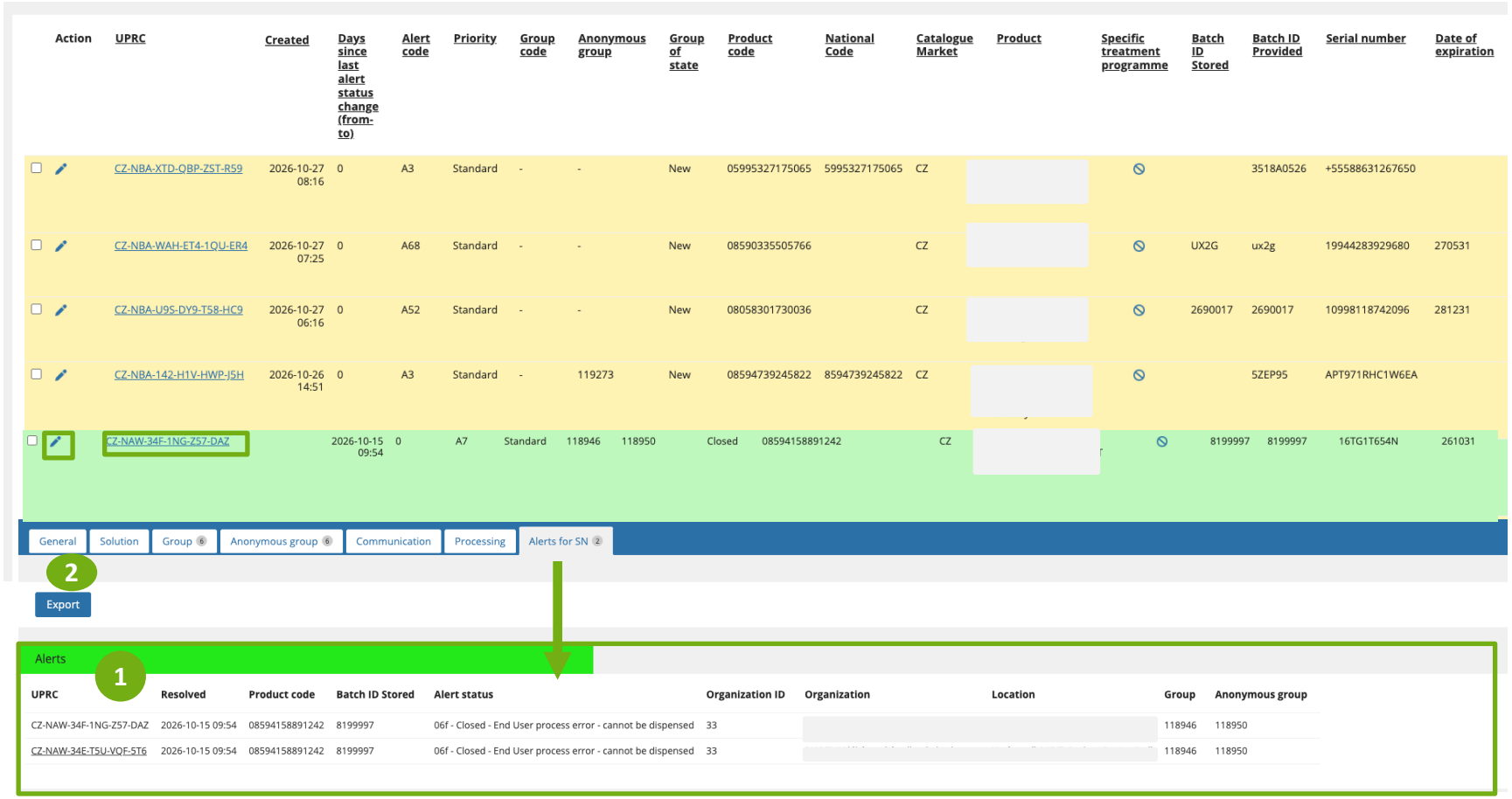
1



ALERTS – ALERT DETAILS – ALERTS FOR SN

If the correct serial number (SN) of a medicinal product is known, the Alert Management System can find and display all alerts generated for that SN.

- This may also help identify the cause of an alert.
- If any such alerts are found, users can view them by clicking the "Alerts for SN" tab in the alert detail. 1
- Alerts for the selected SN can be exported by clicking "Export" (CSV, XLSX). 2
- Access restrictions apply: for locations outside your organisation, the location ID, location name and anonymous group ID are not displayed. Links open only alerts you are authorised to access.



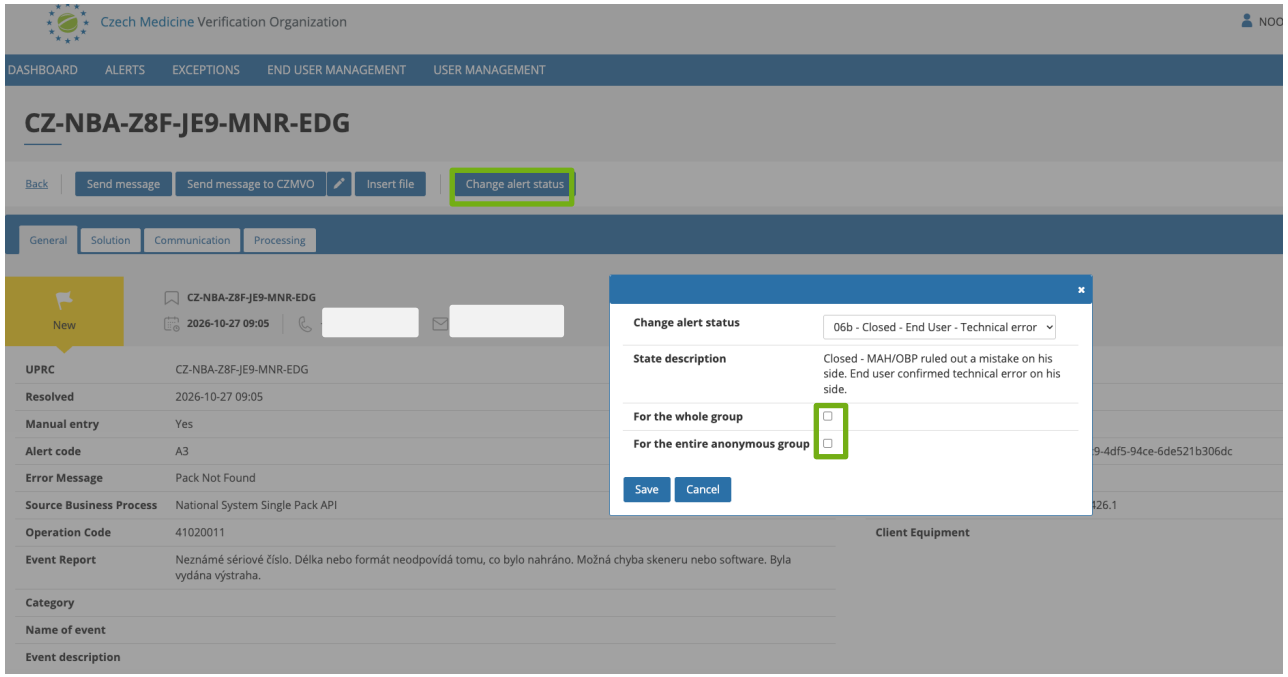
ALERTS – ALERT STATE CHANGE

The “**Change alert status**” button allows you to change an alert’s status. Clicking it opens a window in which you can select the required new status.

Select “**For the whole group**” to apply the new status to all alerts belonging to the same group.

Select “**For the entire anonymous group**” to apply the new status to all alerts belonging to the same anonymous group.

Warning: Before changing the status of an entire alert group, **check that all alerts have the same cause and resolution. Grouping is an automatic function**, and alerts with different causes may be assigned to the same group. If you find that some alerts do not belong in the group, you can remove them using “**Remove from group**”.



Note: The statuses of alerts within a group cannot be changed in bulk if the workflow does not permit at least one alert to change from its current status to the required status. If even one such alert exists, the requested status change will not be performed.

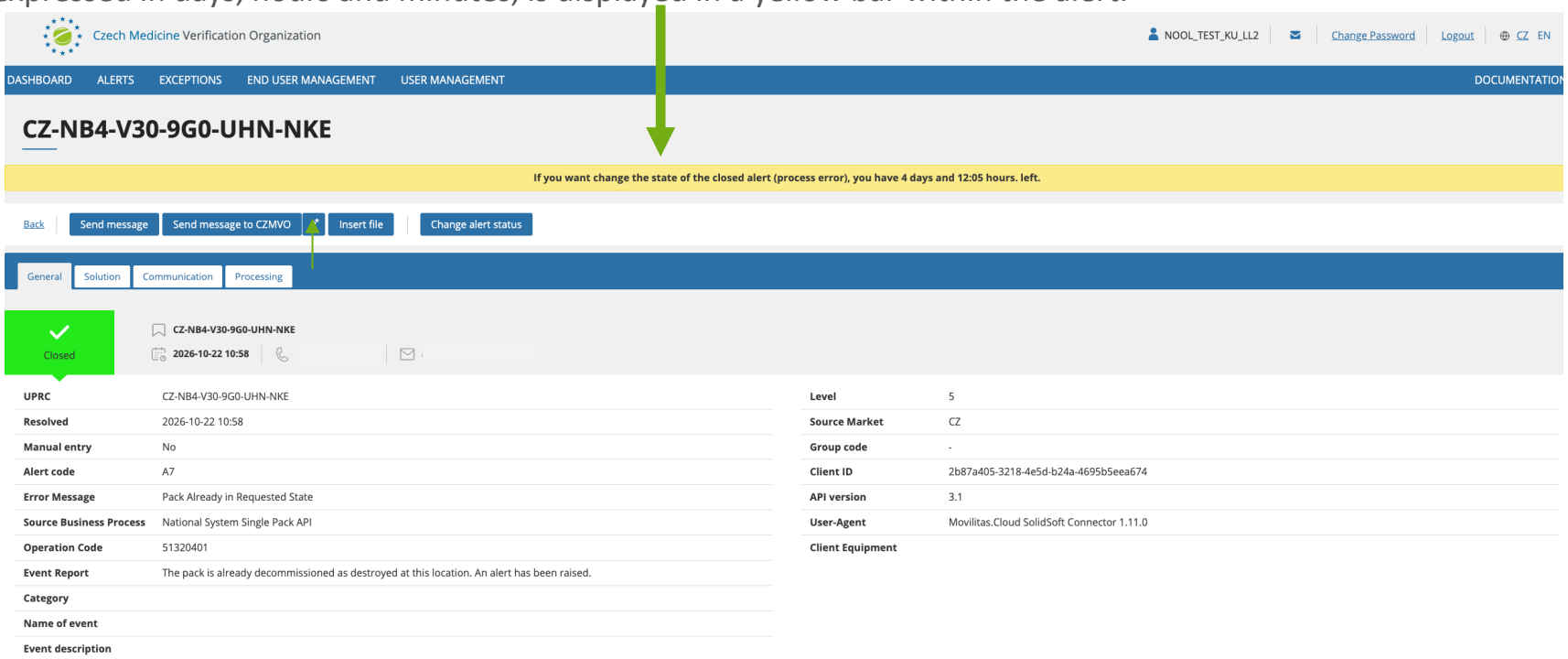
If you also want to send messages to MAH regarding alerts in the group, use the “**Send message**” button. Depending on the message type, this can also change the status of all alerts in the selected group.

Possible alert statuses and the usual procedures for resolving them are provided at the end of this user guide, together with the complete CZAMS alert status code list.

ALERTS — REMAINING TIME TO CHANGE AN ALERT CLOSED BY MAH

If the end user (pharmacy or wholesaler) does not close a process error alert (code **A7** or **A24**) within **48 hours of its generation**, MAH may close the alert on its side after this period. In this situation, however, the end user has a further **9 days** to change the alert status and supply the pack, where permitted.

The remaining time, expressed in days, hours and minutes, is displayed in a yellow bar within the alert.



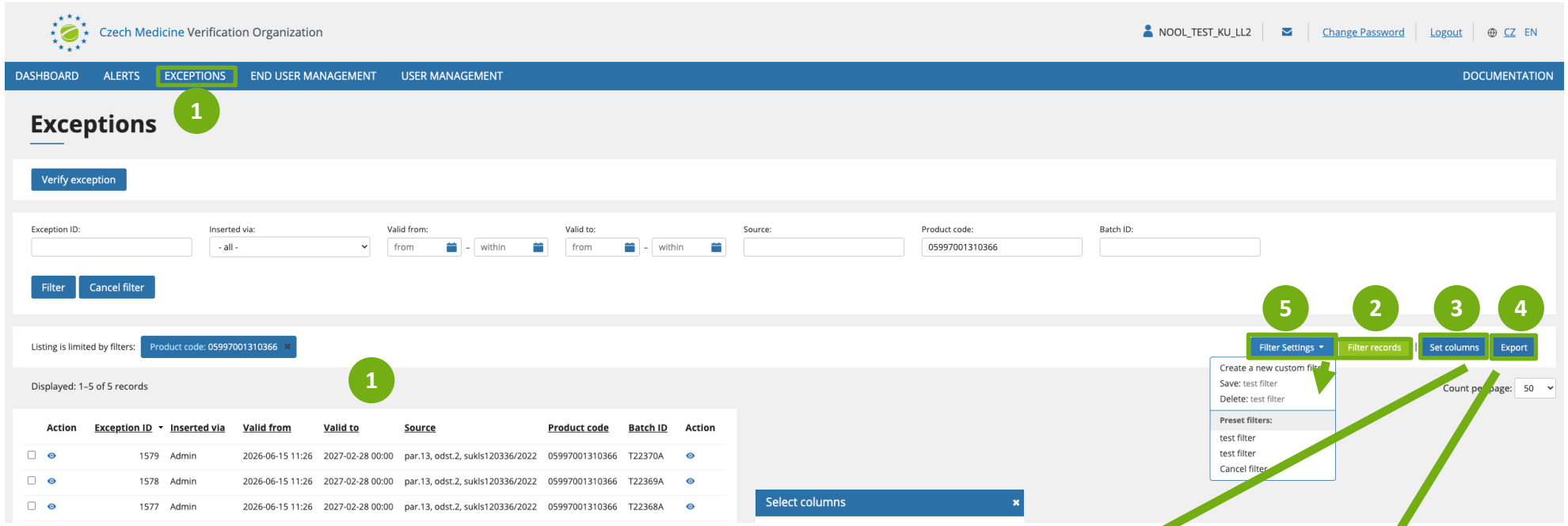
EXCEPTIONS

Exceptions for medicinal products granted by the Ministry of Health under Sections 11r and 13r of the Medicines Act allow **products to be supplied even if the verification result is negative.**

The exception list is created and maintained by CZMVO using SIDC and Ministry of Health data. However, **MAH/OBP is responsible for its completeness and accuracy.**

MAH and CZMVO can add to and update the list on an ongoing basis.

Click 1 **"Exceptions"** to display the **Exception list.**



The exception list can be filtered by 2 clicking the filter control. As with other lists, you can create and manage your own preset filters for faster searching. 5

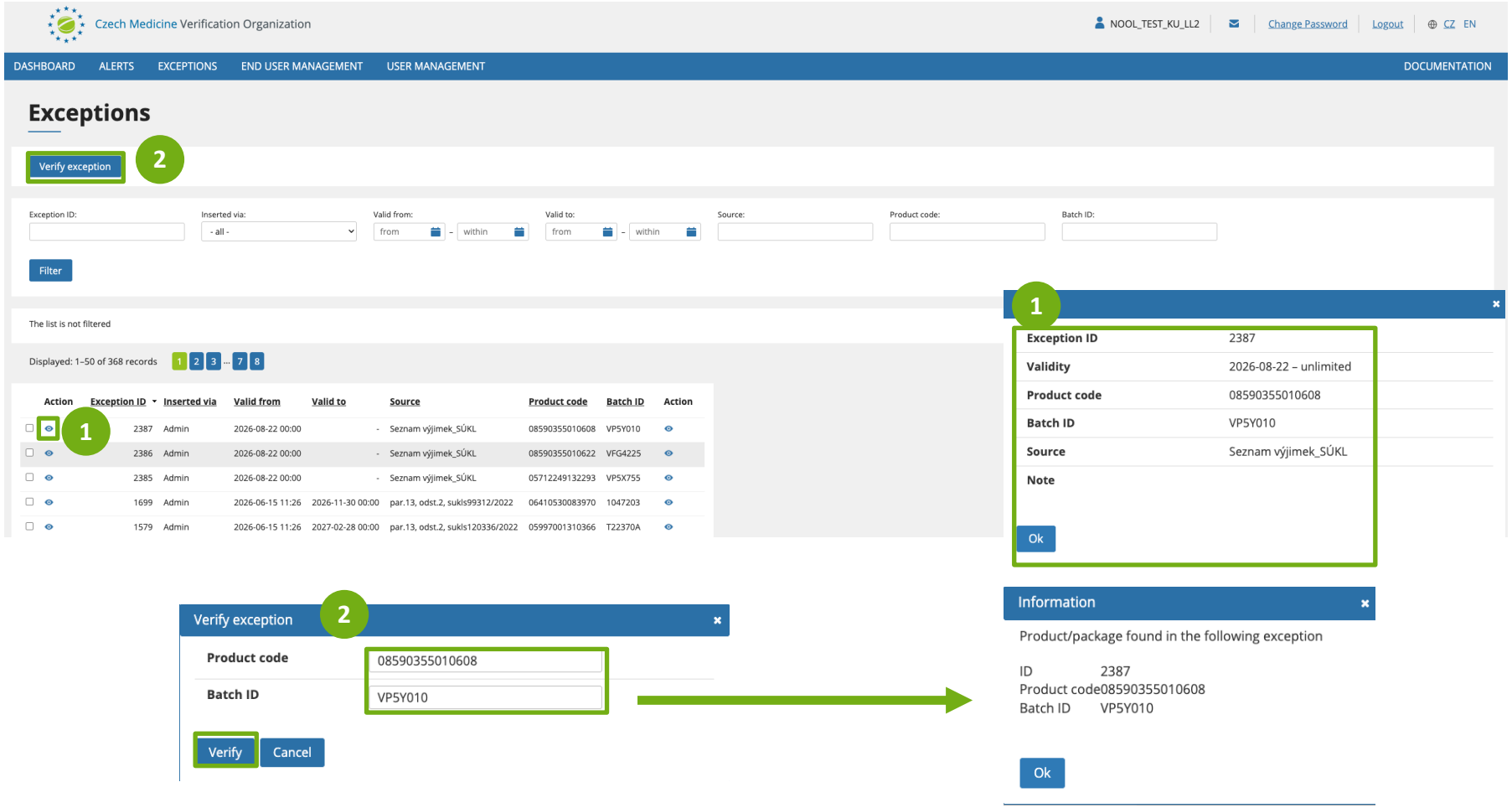
Click 3 "Set columns" to choose which columns are displayed in the list.

Click 4 "Export" to export the exception list according to the criteria selected from the drop-down menus.

EXCEPTIONS – VERIFY EXCEPTION OF A MEDICINAL PRODUCT

Click the 1 „eye icon“ to display detailed information about the exception.

- You can also check whether a Ministry of Health exception applies to the medicinal product.
- Click 2 “Verify exception” to open a form. Enter the product code and batch, then click “Verify” to confirm.
- If the product and batch are found in the exception list, a message confirming a match is displayed. Otherwise, a message indicating that no match was found is displayed.



Part IV

Supplementary information

END USER PROCEDURAL ERRORS

- ✓ After an investigation and **fulfilment of the conditions** approved by SIDC, CZAMS allows a medicinal product to be supplied even following an end user procedural error (pharmacy or wholesaler). This solution is available in CZAMS only For the "**End-User**" role, for **End-User transactions**, for **open** alerts **A7** and **A24**, when the alert is in a **workflow status** that allows the end user to **change the status** or send a preset **message**. **Resolving** and **closing** a procedural error using this tool may allow the **pharmacy or wholesaler to supply the medicinal product immediately**, without CZMVS verification.

  Note: **MAH/OBP** may close end user process errors with status "*06f - Closed - End User process error - cannot be dispensed*" only after **two days** have elapsed since the alert was generated, provided that the end user has not resolved the alert in the meantime.

- ✓ If the **end user** knows that they caused a process error that can be documented under SIDC rules and may ultimately permit supply, they can reopen an alert already closed with status "*06f - Closed - End User process error - cannot be dispensed*". After the required process validation, the end user can change the status to "*06m - Closed - End User process error – the pack can be supplied*". This change can be made within **nine days** after the alert was changed to status 06f.

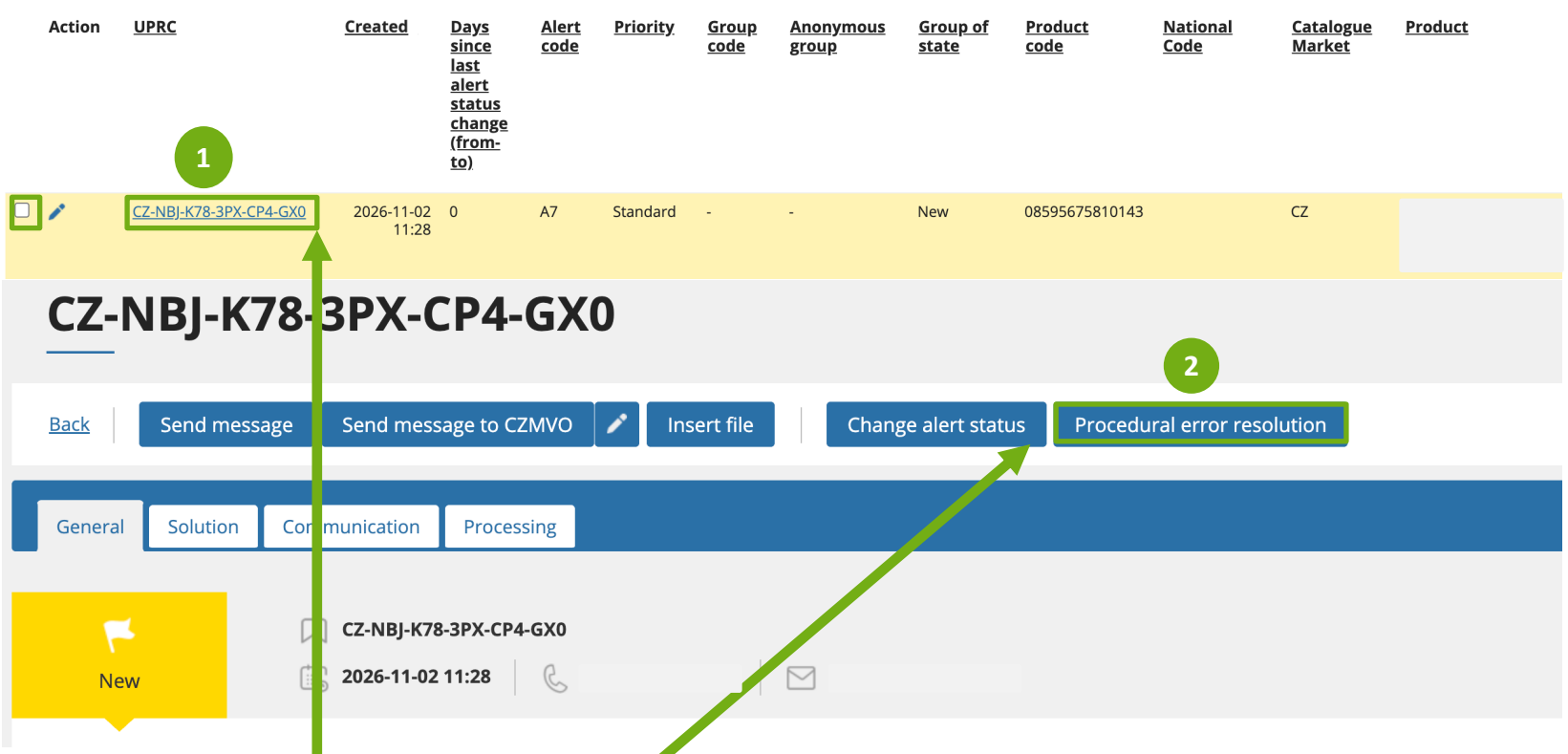
END USER PROCEDURAL ERRORS

A pack transaction in CZMVS can only be performed if the status of the unique identifier is **Active**. If a pack is incorrectly supplied or decommissioned, its unique identifier is permanently deactivated and any further attempt for a pack state change will generate an alert*

In such cases the end user may close the alert if caused as a result of a procedural error that the end user is aware of and eventually they may dispense the pack to public on the condition that the **root cause is well-documented** and details are communicated via CZAMS**

*with the exception of reactivation as per article 13 of COMMISSION DELEGATED REGULATION (EU) 2016/161

**This direction has been approved by SIDC



Resolution procedure:

1. Click the alert's **UPRC** or the „**pencil icon**". A **page displaying all available details about the alert will open.**

2. Click the "**Procedural error resolution**" button.

END USER PROCEDURAL ERRORS

1. Select **“UI deactivation place”.*** This is the original location where the unique identifier was decommissioned, causing the alert at the current location.

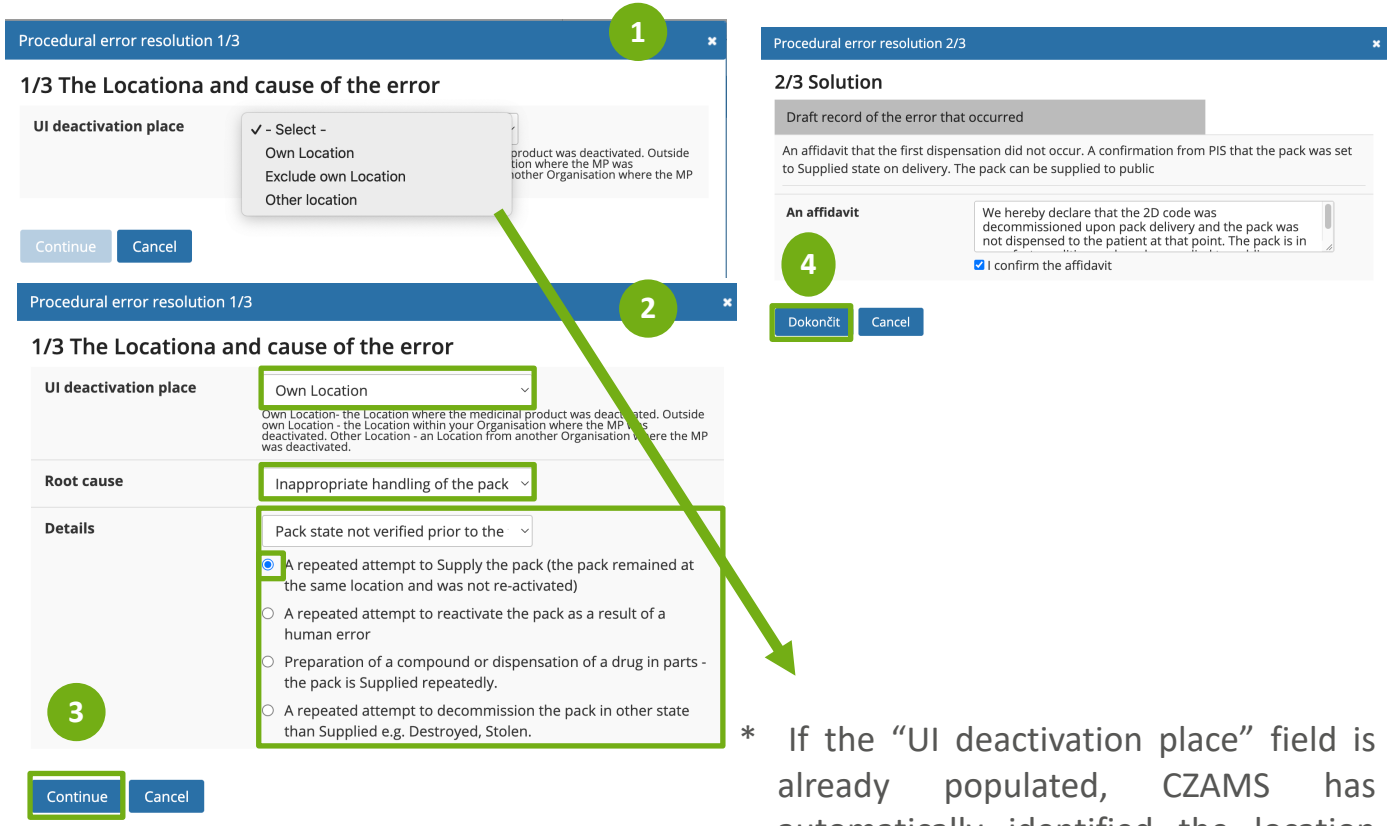
   UI deactivation place:

   a) **Your own Location** — decommissioned at the current location.
   b) **Outside your own Location** — decommissioned at another location within your organisation.
   c) **External site** — decommissioned at a location outside your organisation.

2. Select the “Root cause” from the available options, then tick the relevant “Details”, i.e. the situation corresponding to the cause of the alert.

3. Click “**Continue**”.

4. If your resolution requires an affidavit, it will be displayed automatically. Confirm it by clicking “**Finish**”.



* If the “UI deactivation place” field is already populated, CZAMS has automatically identified the location where the alert originated from the pack audit trail. In this case, skip this step.

Note: A complete overview of the causes and procedures for resolving each type of process error is provided in the table in section 17.2.

END USER PROCEDURAL ERRORS

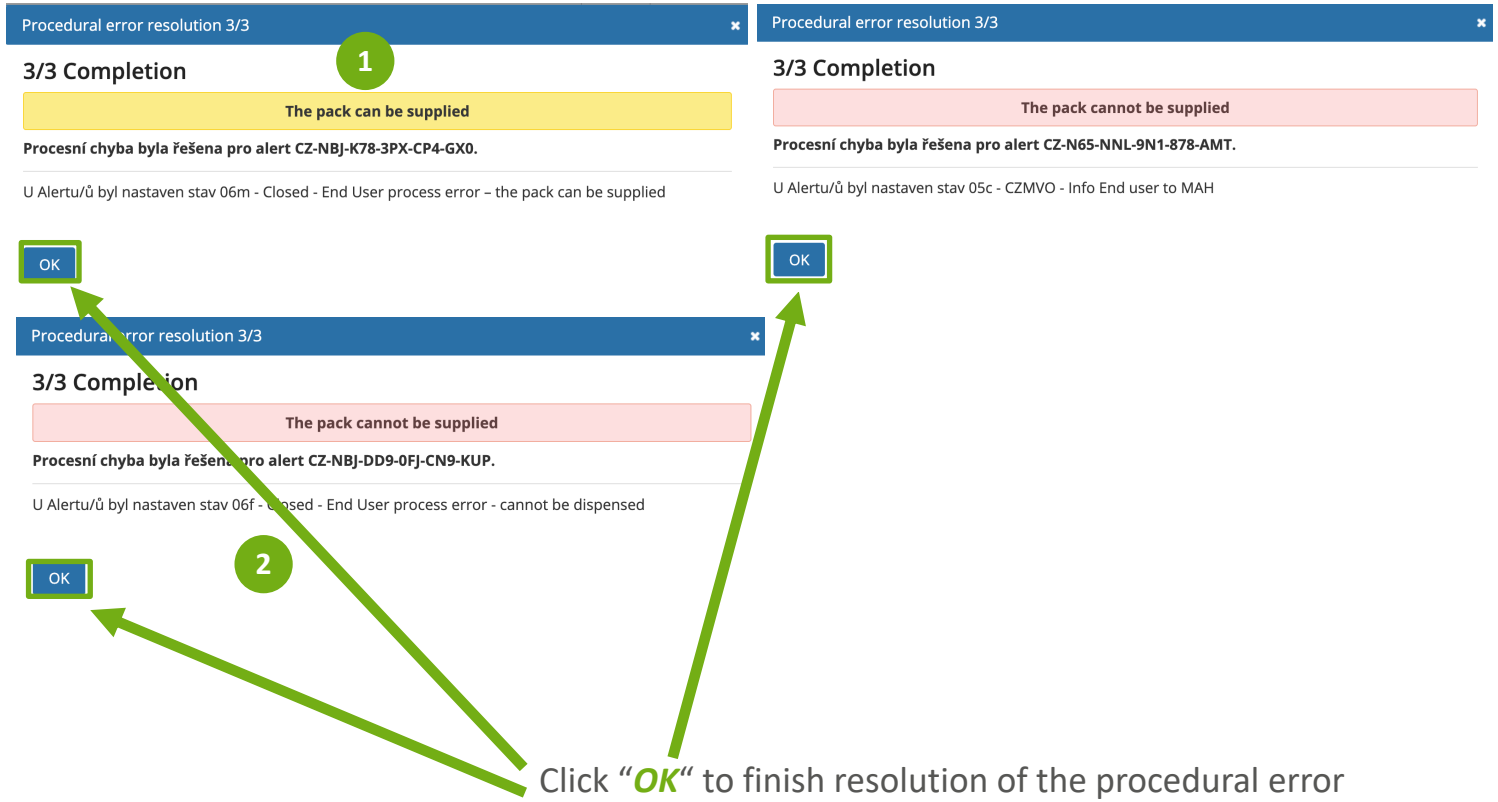
Pay attention to the displayed outcome of the process error resolution. The following resolution outcomes are possible:

1. **"The pack can be supplied" —** The alert is closed with status "06m - Closed - End User process error – the pack can be supplied". The alert is closed and the pack can be supplied to the public.

2. **"The pack cannot be supplied" —** The alert is closed with status "06f - Closed - End User process error - cannot be dispensed". The alert is closed, but the pack cannot be supplied to the public.

3. **"The pack cannot not be supplied"** — to be verified by CZMVO — The alert changes to status "05c - CZMVO - Info End user to MAH". The alert is referred to CZMVO for further investigation.

Note: This situation occurs if the unique identifier was incorrectly decommissioned at another location.



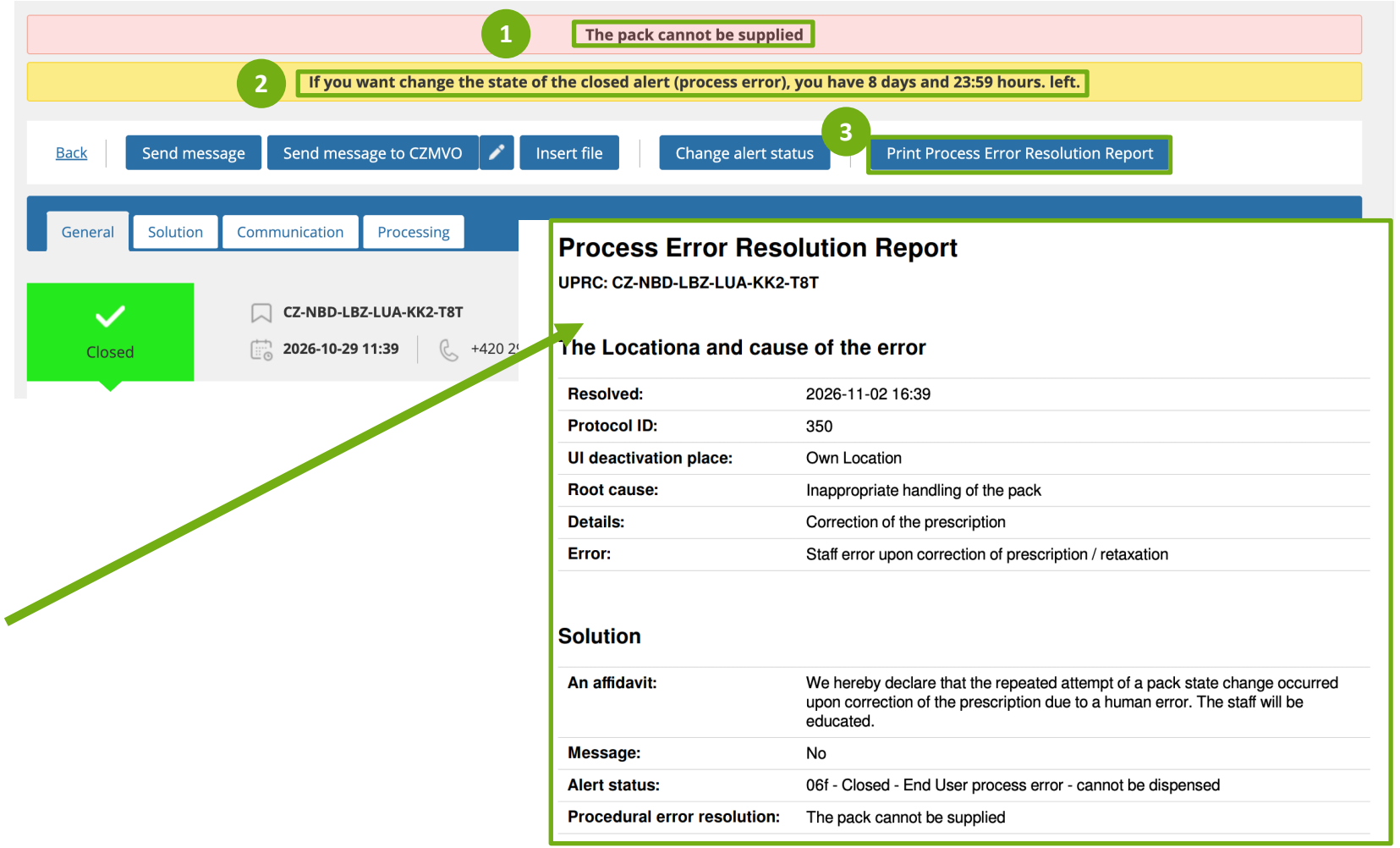
PRINT PROCEDURAL ERROR RESOLUTION REPORT

1. The outcome of the process error closed by the user is displayed in the top bar.

2. If the user's process error resolution can be corrected, the bar shows the remaining time (days, hours and minutes) during which this is possible.

3. Click "**Print Process Error Resolution Report**" to view the outcome of the end user's process error investigation and, if required, print it as a PDF for internal documentation purposes.

   A PDF entitled "*Process Error Resolution Report*" opens in a new window. It can then be printed or saved to your computer.



PROCEDURAL ERRORS – COMPLETE OVERVIEW

Root cause	Details	Examples	Dispensation of the pack to the public
Delayed system response	**Your own text (optional)**	A repeated attempt of a pack state change (e.g. Supplied, Active) due to a delayed response from CZMVS.	can be supplied
Pharmacy information system (PIS) error	**Correction of the prescription**	SW (PIS) error occurs upon correction of the prescription / retaxation / stocktaking - SW (PIS) re-executes the Supplied transaction.	cannot be supplied!
	Your own text (mandatory)	Other error caused by pharmacy information system (PIS)	can be supplied
Inappropriate handling of the pack	**Pack state not verified prior to the transaction**	A repeated attempt to Supply the pack (the pack remained at the same location and was not re-activated)	can be supplied
		A repeated attempt to reactivate the pack as a result of a human error	can be supplied
		A repeated attempt to decommission the pack in other state than Supplied e.g. Destroyed, Stolen.	cannot be supplied!
		Preparation of a compound or dispensation of a drug in parts - the pack is Supplied repeatedly.	can be supplied
	Correction of the prescription	Staff error upon correction of prescription / retaxation	cannot be supplied!
	Stocking error	Mixing of active packs (available for dispensation) with reserved packs (set as Supplied already)	can be supplied
		An attempt to Supply a pack intended for disposal(the current state of the pack is Destroyed)	cannot be supplied!
		An attempt to Supply a pack set to Destroyed state accidentally. The pack is NOT intended for disposal and the Destroyed state was set by error. Any attempt to supply the pack will hence raise an alert	can be supplied
	Returned pack	An attempt to set a pack returned by the patient to Destroyed (the current state is Supplied)	cannot be supplied!
		A pack returned by the patient was erroneously mixed with active drugs in stock and an attempt to Supply the pack occurred. (Illegal activity!)	cannot be supplied!
	Pack transferred outside of the current location	The pack was transferred between locations of the same organization and decommissioned by the originating location.	cannot be supplied!
		The pack brought in by the patient was mistakenly decommisioned during the prescription correction/retaxation.	
		The pack of the medicinal product was incorrectly decommissioned as "Dispensed" by the distributor, in violation of Article 23 of Regulation (EU) 2016/161. A repeated attempt to dispense the product by the hospital/pharmacy triggered an alert.	
		The pack was transferred between locations of a different organization and decommissioned by the originating location.	

ALERT MANAGEMENT SYSTEM — CHANGES

CZAMS Release 9.0 includes the following key changes:

SECURITY

- Invitations to the CZMVO information system are now valid for a limited period: 96 hours / 4 days.

DATA INTEGRATION

- SIDC data on MAHs, sites and medicinal products is now downloaded automatically through the API instead of being processed manually.
- Specific Treatment Programmes (SLP) are now also processed. The “SLP” flag is displayed in the catalogue and the alert detail.
- Exceptions under Section 13r are also processed and handled in the same way as exceptions under Section 11.

NOTIFICATIONS

- Confirmation that the registration email has been sent, and an indication if the email is returned as undeliverable.

PRE-ANALYSIS

- All alerts for a particular serial number (SN) can be displayed in the alert detail.
- If uploaded MAH/OBP data is probably missing (alert code A3), an automatic notification is sent to MAH.
- Technical errors are now automatically closed for “VERIFY” as well as “SUPPLY”. Processing of alerts generated outside the Czech Republic (IMT Fulfilling) has also been added.

REPORTS

- Users with the SIDC role can generate all their reports directly from CZAMS using preset parameters.
- The IN1 report (Pack not Found) automatically completes the serial number and closes the alert if verification is successful.
- Additional product, batch, organisation and site information is automatically retrieved for the alert.
- The alert list export has been redesigned, with additional columns and exports of supplementary tables.

ALERT MANAGEMENT SYSTEM — CHANGES

WORKFLOW AND DASHBOARD

- A new Parallel Distributor (PD) transaction has been added with status “01ba — New — PD transaction”.
- Summary information has been redesigned, and a new “Pending requests” chart has been added to the Dashboard.

USER INTERFACE

- Each user can save their own filter sets in the alert list.
- “Communication history” has been renamed “Communication” and merged with messages (Messenger). “Process workflow” is now under “Processing”.
- New unread-message indicator, copying API keys to the clipboard, XLS/XLSX attachments, and printing process error reports.

BUG FIXES

- Incorrect identification of an “external location” when closing procedural errors has been corrected.
- Duplicate display of messages in alert communication has been removed.

PART V

Alert Statuses and Their Resolution

ALERT RESOLUTION — TERMS

- **CZAMS pre-investigation =** Classification of alerts by their origin: MAH/OBP, parallel distributor, pharmacy or wholesaler. IMT alerts are identified, and a possible cause is suggested, such as a specific end user technical or process error, or an MAH error. An exception under Section 11r of the Medicines Act or priority classification of the alert is assessed.
- **Intermarket alerts =** Alerts generated in a country other than the country where the medicinal product pack is physically verified. “IMT initiating market” — the product is verified in the country concerned, while its data is held in another country’s system. The initiating market must ensure that the alert is fully investigated. “IMT fulfilling market” — the data is held in the country’s system, such as CZMVS, while the pack is physically verified in another country. Such alerts are automatically closed by CZMVO in CZAMS and investigated outside the Czech Republic, in the country where they originated.
- **Priority (emergency) alerts =** Alerts requiring immediate investigation. They are flagged in CZAMS, and MAH, CZMVO staff and the end user are immediately notified when a priority alert is generated. SIDC must be informed in advance before a product is assigned this designation, for example COVID-19 vaccines.
- **End user procedural error** = Most commonly caused by incorrectly configured operational processes, human error or end user actions that do not comply with applicable legislation.
- **End user technical error =** Most commonly caused by incorrect scanner settings or poor scanner quality. In isolated cases, the end user’s software may also cause errors.

CZMVO PRE-ANALYSIS

As part of alert pre-analysis, CZMVO provides information to support further investigation and suggests a possible cause of the alert.

Name	Situation assessed during pre-analysis	Further resolution options — MAH/OBP
EU – Not subject to FMD	The medicinal product is outside the scope of FMD, although its packaging bears a 2D Data Matrix code.	
EU – N/A	End user transaction; pre-analysis has not identified a cause.	
EUT - Date	Suspected incorrect reading of the expiry date.	For the technical-error cases, MAH/OBP continues investigating and closing the alert in cooperation with the end user, either confirming the cause or identifying another one. Alternatively, the end user may complete the investigation directly, close the alert with status “06b - Closed - End User - Technical error” and verify the medicinal product pack again before supply.
EUT - Long string in Serial number	Likely end user technical error. Suspected incorrect scanner settings resulting in a long SN string.	
EUT - Caps Lock	Likely end user technical error. Suspected unhandled keyboard issue involving Caps Lock.	
EUT - Incorrect chain length in batch	Likely end user technical error. Suspected incorrect scanner settings resulting in an incorrect batch number length.	
EUT - EN/CZ	Likely end user technical error. Suspected unhandled keyboard layout issue involving English/Czech settings.	

CZMVO PRE-ANALYSIS

As part of alert pre-analysis, CZMVO provides information to support further investigation and suggests a possible cause of the alert.

Name	Situation assessed during pre-analysis	Further resolution options — MAH/OBP
EUT - Short character string in Serial number	Likely end user technical error. Suspected incorrect scanner settings resulting in a short SN string.	For the technical-error cases, MAH/OBP continues investigating and closing the alert in cooperation with the end user, either confirming the cause or identifying another one. Alternatively, the end user may complete the investigation directly, close the alert with status “06b - Closed - End User - Technical error” and verify the medicinal product pack again before supply.
EUT - Character mismatch - SN	Likely end user technical error. Suspected poor scanner quality causing character substitutions such as O/0, E/3 or I/L.	
EUT - Character mismatch - batch ID	Likely end user technical error. Suspected poor scanner quality causing character substitutions such as O/0, E/3 or I/L.	
EUT - incorrect length and SN format	Likely end user technical error. Suspected incorrect scanner settings resulting in incorrect SN length and format.	
EUT - incorrect length and batch format	Likely end user technical error. Suspected incorrect scanner settings resulting in incorrect batch number length and format	

CZMVO PRE-ANALYSIS

As part of alert pre-analysis, CZMVO provides information to support further investigation and suggests a possible cause of the alert.

Name	Situation assessed during pre-analysis	Further resolution options — MAH/OBP
EUT - Fixed, supplied	End user technical error. According to the audit trail, the pack was subsequently successfully verified and supplied.	The alert was automatically closed following an audit trail check. No further action is required from MAH/OBP
EUT - Fixed, verified	End user technical error. According to the audit trail, the pack was subsequently successfully verified.	The alert was automatically closed following an audit trail check. No further action is required from MAH/OBP.
EUT - Duplication in bulk operation	Two identical serial numbers were scanned during a bulk operation.	MAH/OBP can close the alert with status “06b - Closed - End User - Technical error”.
EUP - Repeated	A repeated pack status change transaction. It is unclear whether the original successful decommissioning was performed at the user’s own location or at an external location.	The end user explains the cause through CZAMS by selecting from the available options, properly documents the case and confirms a affidavit. If the end user does not close the alert within 48 hours of its generation, the alert becomes available to MAH, which may then close it on its side.
EUP - Repeated - This location	A repeated pack status change transaction at the same site. The pack was previously successfully decommissioned at that location.	
EUP - Repeated – Outside Your Organization	A repeated pack status change transaction. The pack was previously successfully decommissioned at an external location belonging to another organisation.	

CZMVO PRE-ANALYSIS

As part of alert pre-analysis, CZMVO provides information to support further investigation and suggests a possible cause of the alert.

Name	Situation assessed during pre-analysis	Further resolution options — MAH/OBP
EUP – Repeated – outside your Locations	A repeated pack status change transaction. The pack was previously successfully decommissioned at another location within the organisation.	The end user explains the cause through CZAMS by selecting from the available options, properly documents the case and confirms an affidavit. If the end user does not close the alert within 48 hours of its generation, the alert becomes available to MAH, which may then close it on its side.
EUP - Unauthorized	An unauthorised pack status change transaction. It is unclear whether the original successful decommissioning was performed at the user's own location or at an external location.	
EUP – Unauthorized – This location	An unauthorised pack status change transaction at the same location. The pack was previously successfully decommissioned at that location.	
EUP – Unauthorised – outside your Organisation	An unauthorised pack status change transaction. The pack was previously successfully decommissioned at an external location belonging to another organisation.	
EUP - Unauthorised – outside your Locations	An unauthorised pack status change transaction. The pack was previously successfully decommissioned at another site within the organisation.	

CZMVO PRE-ANALYSIS

As part of alert pre-analysis, CZMVO provides information to support further investigation and suggests a possible cause of the alert.

- Alert codes: All

Name	Situation assessed during pre-analysis	Further resolution options — MAH/OBP
MAH - Batch is not uploaded in CZMVS	Suspected missing data in the repository.	MAH/OBP checks whether the data uploaded to the repository is correct and takes corrective action where necessary. If an MAH/OBP error is confirmed, the alert can be closed with status “06a - Closed - MAH error - Fixed” or “06c - Closed - MAH error- Not fixed.
MAH - exception 11r	MAH error covered by an exception under Section 11r of the Medicines Act.	MAH/OBP can close the alert with status “06d - Closed - MAH error - MH exception”. CZMVO can also close it in CZAMS.
MAH – Exception under 13r	MAH error covered by an exception under Section 13r of the Medicines Act.	MAH/OBP can close the alert with status “06d - Closed - MAH error - MH exception”. CZMVO can also close it in CZAMS.
NMVS error - Alert older than 365 days	An open Level 5 alert generated more than 365 days ago.	

INITIAL ALERT STATUSES

Alert statuses in CZAMS and subsequent actions by CZMVS users.

- Alert codes: **All**

Status code and title	End user procedure	MAH/OBP procedure
01a (aa) - New - End User transaction	Keep the medicinal product pack in quarantine until the investigation is completed.	Upon receiving notification of the alert, MAH/OBP should immediately begin investigating its possible cause.
01c - Unknown MAH	Provide information about the MAH, either directly within the alert using "Send message to CZMVO" or by emailing support@czmvo.cz.	
02a - Investigation - End user transaction	Keep the medicinal product pack in quarantine until the investigation is completed.	MAH may use this status, but it is optional. By setting it, MAH informs CZMVO through CZAMS that the alert is being investigated. If resolution takes longer, MAH will therefore not receive escalation emails after 5 or 10 days of inactivity.
02c - CZMVO - Investigation MAH	Provide information about the MAH, either directly within the alert using "Send message to CZMVO" or by emailing support@czmvo.cz.	

ALERT ESCALATION STATUSES

Alert statuses in CZAMS and subsequent actions by CZMVS users.

- Alert codes: **all; statuses 03f and 03g apply only to A7 and A24.**

Status code and title	End user procedure	MAH/OBP procedure
03a - MAH/End User - unclosed alert older than 5 days	Keep the medicinal product pack in quarantine until the investigation is completed.	MAH has received an email notification from CZAMS that the alert has remained in "MAH — New" status for 5 days.
03b - MAH/End User - unclosed alert older than 10 days	Keep the medicinal product pack in quarantine until the investigation is completed.	MAH has received an email warning from CZAMS that the alert has remained in "MAH — New" status for 10 days.
03c - End user - MAH request - Inactivity 48 hours	Keep the medicinal product pack in quarantine until the investigation is completed.	MAH has sent a request for additional information to the end user through a CZAMS message, selecting from several predefined message options
03d - End user - Inactivity 5 days	Keep the medicinal product pack in quarantine until the investigation is completed.	MAH has sent a request for additional information to the end user through a CZAMS message, selecting from several predefined message options.
03f - End User- process error - not closed 5 **03g - End User- process error - not closed 10 days**	The end user is notified of inactivity. The end user identifies the cause, documents the event, selects the relevant options in CZAMS and confirms a declaration of honour. Keep the medicinal product pack in quarantine until the investigation is completed.	MAH can change the alert status once 48 hours have elapsed since its generation. The alert can be closed with status "06f - Closed - End User process error - cannot be dispensed".

Reported to SIDC after 30 days.

Reported to SIDC after 30 days.

INTERMEDIATE ALERT STATUSES

Alert statuses in CZAMS and subsequent actions by CZMVS users.

- Alert codes: **All**

Status code and title	End user procedure	MAH/OBP procedure
04a - MAH - info from End user	Keep the medicinal product pack in quarantine until the investigation is completed. The end user receives a message requesting the information required by MAH for the investigation.	MAH has sent a request for additional information to the end user through a CZAMS message, selecting from several predefined message options.
04b - MAH/End User - Info from CZMVO	Keep the medicinal product pack in quarantine until the investigation is completed.	MAH has sent a request for additional information to CZMVO through a CZAMS message, either using a custom message or selecting a predefined message.
04d - CZMVO - Info from end user - MAH unkown	Provide information about the MAH, either directly within the alert using “Send message to CZMVO” or by emailing support@czmvo.cz.	
05a - End user - Info to MAH **05b - CZMVO - Contacts end User** **05c - CZMVO - Info End user to MAH** **05d - CZMVO - Info to MAH/End User**	Keep the medicinal product pack in quarantine until the investigation is completed. Provide the information requested by MAH or CZMVO during the investigation and, where necessary, communicate with the CZMVO support team.	MAH receives the requested information from the end user or CZMVO through CZAMS.

FINAL ALERT STATUSES

Alert statuses in CZAMS and subsequent actions by CZMVS users.

- Alert codes: **A2, A3, A52, A68.**
- During the investigation, MAH/OBP should check the data uploaded to EMVS/CZMVS. If one of the causes listed under "Most common alert causes" is identified, follow the recommended MAH/OBP procedure. The recommended end user procedure is also provided.

Status code and title	Most common alert causes:	End user procedure	MAH/OBP procedure
06a - Closed - MAH error - Fixed	• Data not uploaded — the batch is missing or has been uploaded incorrectly. • IMT failure — an incorrect batch number prevents the batch from being found in the foreign repository. • System timeout — the batch is not found because the query response is not received within the required time limit. • Incorrectly uploaded batch number. • Data not uploaded — serial numbers are missing or have been uploaded incorrectly. • System timeout — the date cannot be verified because the query response is not received within the required time limit. • The manufacturer uploaded incorrect Product Pack Data to the EU Hub. • The batch number is read instead of the expiry date.	Keep the medicinal product pack in quarantine until the investigation is completed. After the alert is closed, CZAMS displays: **Corrected — verification can be repeated! Release from quarantine. The pack may be supplied after successful verification. If verification fails again, return the pack to quarantine with the new alert ID, provided that fewer than 14 days have elapsed since quarantine began for the original alert. Otherwise, after 14 days in quarantine without resolution, return the pack to the supplier, quoting the alert ID.**	Once MAH/OBP has corrected and properly uploaded or supplemented the batch data through the EU Hub to EMVS/CZMVS and closed the alert with this status, the end user can verify the pack again and then release it from quarantine and supply it to the patient.

FINAL ALERT STATUSES

- Alert codes: **A2, A3, A52, A68**. During the investigation, the end user should, where possible, check for technical errors or causes on their side. These are most commonly related to incorrect scanner settings, errors in the end user's verification application or scanning technique. If one of the following causes is identified, follow the recommended procedure.

Status code and title	Most common alert causes:	End user procedure	MAH/OBP procedure
06b - Closed - End User - Technical error	• Rapid scanning causes the batch number to be combined with the GTIN or SN, the batch number to be read twice, or data from multiple packs to be combined. • The SN is too short (truncated), too long (including part of another data field), or contains invalid characters. • Incomplete or incorrect scanning — an incomplete number or a product code appended to the batch number. • Y/Z substitution or changes in letter case caused by Caps Lock being enabled or Shift being pressed during scanning. Y/Z substitution results from a keyboard layout different from the one configured for the scanner, typically English/Czech or QWERTZ/QWERTY. • Incorrectly configured scanners transmit an incorrect batch identifier. • Incorrect manual entry, such as confusion between 1 and l, or O and 0. • Incorrect use of separators shifts parts of a number or other characters into the batch number. • End user systems convert the expiry date, for example from 210600 to 210531 or 2510631. This no longer occurs in the Czech Republic. • Incorrect repeated manual data entry or manual entry of the printed expiry date in MM/YY format.	The end user should take appropriate corrective action to address the cause of the alert: • Scan the pack again after a short interval following the previous verification. • Disable Caps Lock before scanning, then scan the pack again. • Switch to the Czech keyboard layout or the correct QWERTZ/QWERTY layout, then scan the pack again. • Arrange with the end user's IT/software provider to modify the software to handle missing separators. • Arrange with the IT/software provider to eliminate expiry date conversion. • Scan the unique identifier again or carefully re-enter all required data manually. Where possible, perform a test scan to check the scanner settings, then return to the pack that generated the alert. **The end user can then verify the pack again and, after successful verification and decommissioning of the unique identifier, release it from quarantine and supply it to the patient.**	MAH also begins an investigation on its side. However, once an end user error is identified, only the end user can correct it. MAH may nevertheless close the alert with this status if the available data demonstrates that an end user error caused it.

FINAL ALERT STATUSES

➢ Alert codes: A2, A3, A52, A68.

During the investigation, MAH/OBP should check the data uploaded to EMVS/CZMVS. If one of the causes listed under "Most common alert causes" is identified, follow the recommended MAH/OBP procedure. The recommended end user procedure is also provided.

Status code and title	Most common alert causes:	End user procedure	MAH/OBP procedure
06c - Closed - MAH error- Not fixed.	• Incorrectly printed code on the pack. • An OBP using "Indian codes" uses a GTIN that it later also used for FMD, resulting in an alert. • Missing separators shift parts of a number or other characters into the batch number. • The manufacturer printed incorrect pack identification data in the 2D code. • The manufacturer printed incorrect pack identification data in human-readable format. • MAH re-uploaded data for packs already distributed. • OBP attempts to change the status of a pack whose unique identifier has already been decommissioned, for example "sample to sample".	Keep the pack in quarantine during the investigation and wait for MAH to close the alert or request additional information. After the investigation is completed and the alert is closed, CZAMS displays: **MAH/OBP error. Cannot be corrected — do not verify again. Return the pack to the supplier, quoting the alert ID.** Return the pack to the wholesaler in accordance with the returns procedure established within the end user's organisation.	Following investigation with OBP, the data cannot be corrected or uploaded correctly, or the incorrectly printed code on the pack cannot be corrected. The batch data cannot be corrected through the EU Hub in EMVS/CZMVS. The pack cannot be supplied to the patient.

FINAL ALERT STATUSES

- Alert codes: **All**

  During the investigation, MAH/OBP should check the data uploaded to EMVS/CZMVS. If one of the causes listed under "Most common alert causes" is identified, follow the recommended MAH/OBP procedure. The recommended end user procedure is also provided.

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06d - Closed - MAH error - MH exception	• Incorrectly printed code on the pack. • An OBP using "Indian codes" uses a GTIN that it later also used for FMD, resulting in an alert. • Missing separators shift parts of a number or other characters into the batch number. • The manufacturer printed incorrect pack identification data in the 2D code. • The manufacturer printed incorrect pack identification data in human-readable format. • MAH re-uploaded data for packs already distributed. • OBP attempts to change the status of a pack whose unique identifier has already been decommissioned, for example "sample to sample".	Keep the pack in quarantine during the investigation and wait for MAH or CZMVO to close the alert. After the investigation is completed and the alert is closed, CZAMS displays: "**Ministry of Health exception under Section 11r or 13r — DO NOT VERIFY. The pack may be supplied. Release from quarantine.**"	During the investigation, **MAH/OBP** must check whether a Ministry of Health exception under Section 11r or 13r of the Medicines Act has been approved for the medicinal product. If an exception has been approved for the product and batch concerned, set the appropriate status in CZAMS. The end user can then release the pack from quarantine and supply it to the patient.

FINAL ALERT STATUSES

- Alert codes: **A7, A24**. During the investigation, MAH/OBP should check the data uploaded to EMVS/CZMVS. If one of the causes listed under “Most common alert causes” is identified, follow the recommended MAH/OBP procedure. The recommended end user procedure is also provided.

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06f - Closed - End User process error - cannot be dispensed	• An end user attempts to decommission an already decommissioned pack a second time. • An attempt to decommission an inactive or expired pack. • Incorrect internal labelling and classification of a pack due to a misunderstanding. • An accidentally repeated operation or incorrect decommissioning of a pack to the wrong status. • Incorrect internal labelling and classification of a pack due to a misunderstanding. • A transfer between pharmacies in which the selling pharmacy incorrectly decommissions the pack as “Supplied”, and the receiving pharmacy generates an alert when attempting to supply it to a patient. • Errors resulting in a request being sent again. • An end user attempts to decommission an already decommissioned pack a second time. • An attempt to decommission an inactive or expired pack. • Incorrect internal labelling and classification of a pack due to a misunderstanding.	Keep the pack in quarantine until the investigation is completed. After the alert is generated, investigate possible process-related causes on the end user’s side. The MAH and CZMVO investigations have confirmed that the error is not attributable to MAH/OBP and have identified an end user process error.* After the investigation is completed and the alert is closed, CZAMS displays: “**No MAH/OBP error. Unable to fix - cannot be re-authenticated. Further procedure according to the internal processes of the organization.”**	During the investigation, the end user or MAH identified an end user process error. These alerts require an explanation and documentation of the cause, preferably in CZAMS. The cause cannot be corrected in CZMVS; another attempt to decommission the unique identifier would therefore generate another alert. It has also been confirmed that the product is not falsified.

FINAL ALERT STATUSES

- Alert codes: **A7, A24**. During the investigation, MAH/OBP should check the data uploaded to EMVS/CZMVS. If one of the causes listed under "Most common alert causes" is identified, follow the recommended MAH/OBP procedure. The recommended end user procedure is also provided.

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06m - Closed - End User process error – the pack can be supplied	• An end user attempts to decommission an already decommissioned pack a second time. • An attempt to decommission an inactive or expired pack. • Incorrect internal labelling and classification of a pack due to a misunderstanding. • An accidentally repeated operation or incorrect decommissioning of a pack to the wrong status. • Incorrect internal labelling and classification of a pack due to a misunderstanding. • A transfer between pharmacies in which the selling pharmacy incorrectly decommissions the pack as "Supplied", and the receiving pharmacy generates an alert when attempting to supply it to a patient. • Errors resulting in a request being sent again. • An end user attempts to decommission an already decommissioned pack a second time. • An attempt to decommission an inactive or expired pack. • Incorrect internal labelling and classification of a pack due to a misunderstanding.	Keep the pack in quarantine until the investigation is completed. After the alert is generated, investigate possible process-related causes on the end user's side. The MAH and CZMVO investigations have confirmed that the error is not attributable to MAH/OBP and have identified an end user process error.* **The end user must document the cause of the process error in accordance with SIDC requirements. By selecting from the available options and following the instructions for the relevant process error, the medicinal product may be released from quarantine and supplied without further verification.** After the investigation is completed and the alert is closed, CZAMS displays: **"Closed - End User process error – the pack can be supplied. The end user has documented the cause".**	During the investigation, the end user or MAH identified an end user process error. These alerts require an explanation and documentation of the cause, preferably in CZAMS. The cause cannot be corrected in CZMVS; another attempt to decommission the unique identifier would therefore generate another alert. It has also been confirmed that the product is not falsified.

FINAL ALERT STATUSES

- Alert codes: **All**. During the investigation, the end user should, where possible, check for technical errors or causes on their side, most commonly associated with incorrectly configured processes, human error or unsuitable software settings. If one of the following causes is identified, follow the recommended end user or MAH procedure.

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06g - Closed - NMVS error	This concerns packs: • Previously successfully supplied in the Czech Republic, for which multimarket data synchronisation was not completed correctly. • Not verified because of a long response time, where the pack status change was not completed correctly.	For an alert generated in the Czech Republic at an end user's site, keep the pack in quarantine during the investigation and wait for MAH or CZMVO to close the alert. After the investigation is completed and the alert is closed, CZAMS displays one of the following messages, depending on the system error: "**CZMVS error — verification can be repeated! Release from quarantine."** **"CZMVS error — verification cannot be repeated! Release from quarantine."**	MAH does not close an alert with this status, but should still investigate it. If no error is found on MAH's side, CZMVO begins its investigation. During the investigation, CZMVO confirmed a data synchronisation error and closed the alert. The pack is not in quarantine, as it was supplied before the alert was generated. This has no impact on medicines on the Czech market. Another possible cause is a long system response time, known as a system timeout: the pack is not found because the query response is not received within the required time limit.
06o - Closed - End User does not cooperate - cannot be supplied	MAH has completed its investigation and repeatedly requested additional information from the end user. The end user is not cooperating. The medicinal product may not be supplied. CZMVO informs SIDC. **Note: This status can only be used after the alert has spent 9 days in status 03d (EU escalation — 5 days).**	Closed by MAH — may not be supplied. The end user has not cooperated despite reminders. CZMVO informs SIDC. Contact CZMVO urgently or respond to the requests from MAH or CZMVO.	Closed — the end user has not cooperated despite reminders — may not be supplied. CZMVO informs SIDC."

FINAL ALERT STATUSES

- Alert codes: **All**
- During the investigation, MAH/OBP should check the data uploaded to EMVS/CZMVS. The end user should check for technical or process errors on their side, after which CZMVO should investigate possible CZMVS system errors. If all these possible causes can be excluded, follow the end user or MAH procedure below

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06h - Suspected Counterfeit!	• All possible technical or other causes attributable to MAH, the end user and CZMVS have been excluded.	Keep the medicinal product pack in quarantine until the investigation is completed. After the investigation is completed and the alert is closed, CZAMS displays: **"The MAH and CZMVO investigations have confirmed a potentially FALSIFIED PRODUCT! The information will be forwarded to SIDC, EMVO, EMA and the European Commission. KEEP THE MEDICINAL PRODUCT PACK SAFE! You will be contacted regarding the next steps."**	The investigation by all parties involved has excluded all other possible causes of the alert. MAH has identified a potentially FALSIFIED PRODUCT. The information will be forwarded to SIDC, EMVO, EMA and the European Commission. Further investigation into the suspected falsification will be conducted in cooperation with MAH and in accordance with the procedures established by the organisation and SIDC.

FINAL ALERT STATUSES

- Alert codes: **All**

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06l - Closed - Non FMD	• The medicinal product is not subject to FMD.	Keep the medicinal product pack in quarantine during the investigation and wait for CZMVO to close the alert.	

FINAL ALERT STATUSES

- Alert codes: **All**

Status code and title	Most common alert causes	End user procedure	MAH/OBP procedure
06z - Closed - Unclosed level 5 alert created 365 days ago	• The alert has not been closed by any party for 365 days.		