EUROPEAN COMMISSION

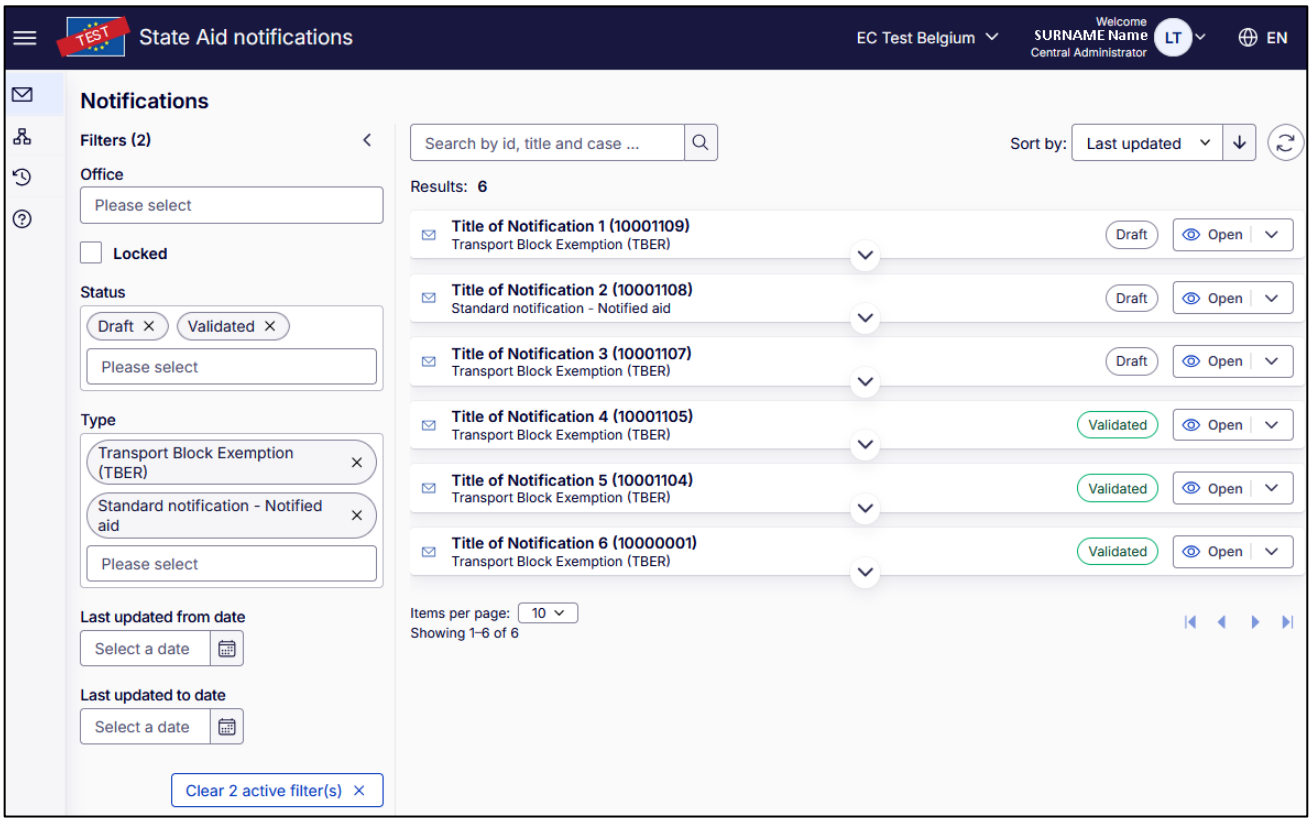
COMPETITION DG

Horizontal Management

Information Technology

eNotifications v1.0.5

User Manual v1.02



1. TABLE OF CONTENTS

1. Table of Contents 2
2. Document History 5
3. Introduction 5
3.1. Purpose of eNotifications 5
3.2. Purpose and scope of this manual 5
3.3. URLs and contact points 5
4. Getting access and support for eNotifications 6
4.1. Who grants access 6
4.2. Access to eNotifications 6
4.3. Required EU Login account 6
4.4. Login, user profiles and homepage 6
4.5. Contact points in your legal entity (Member State) 7
5. User profiles and permissions 8
5.1. User profiles involved in access management 8
5.1.1. Central Administrators 8
5.1.2. Local Administrators 8
5.2. User profiles involved in submitting notification forms 9
5.2.1. Encoder 9
5.2.2. Signatory 10
5.2.3. Pre-validator 10
5.2.4. Validator 10
5.2.5. Viewer 10
6. The Access Management Module 10
6.1. Managing the Member State (Legal Entity) 11
6.1.1. Editing Legal Entity 'Details' 11
6.1.2. Setting for default read-only access for Central and Local Administrators 12
6.1.2.1. Default read-only notification access is enabled 12
6.1.2.2. Default read-only notification access is disabled 13
6.2. Office management 14
6.2.1. Create an Office 15
6.2.2. Update an Office 16
6.2.3. Assign users to an Office 16
6.2.3.1. Assign users to an Office from the 'Offices'-tab 16
6.2.3.2. Assign user to an Office from the 'Users'-tab 18
6.2.4. Remove users from an Office 20
6.2.5. Disable or enable an Office 20
6.2.5.1. Disable an Office 20
6.2.5.2. Enable an Office 21
6.3. Group management 22
6.3.1. Create a Group 22
6.3.2. Update a Group 23
6.3.3. Assign users to a Group 24
6.3.3.1. Assign users to a Group from the 'Groups'-tab 24
6.3.3.2. Assign user to a Group from the 'Users'-tab 25

6.3.4. Remove users from a Group 26
6.3.5. Disable or enable a Group 27
6.3.5.1. Disable a Group 27
6.3.5.2. Enable a Group 28
6.4. User management 29
6.4.1. Create a user 29
6.4.1.1. Scenario 1: the new user has an EU Login account 30
6.4.1.2. Scenario 2: the new user does not have an EU Login account 31
6.4.1.3. Scenario 3: the user already has access to eNotifications 33
6.4.1.4. Specifics when assigning the Validator profile to a user 33
6.4.2. Update user details 34
6.4.2.1. How to update a user's e-mail address or name 35
6.4.3. Disable or enable a user 36
6.4.3.1. Disable a user 36
6.4.3.2. Enable a user 37
6.5. Reassigning or sharing assignments between users 38
6.6. 'Audit trails' in the Access Management Module 39
7. The Notifications Module 41
7.1. Search function and filters available in the Notifications module 41
7.2. Creating a notification 43
7.2.1. Creating a block exempted notification (GBER, ABER, FBER, TBER) 43
7.2.2. Creating a simplified notification 43
7.2.3. Creating a standard notification 44
7.2.3.1. Providing a SA reference / Case number 44
7.2.3.2. Selecting the standard notification 'variant' (pre-notification, notification, legal certainty) 45
7.3. Setting up a Notification Team 46
7.3.1. The notification team overview 46
7.3.2. Assigning users to a notification team 48
7.3.2.1. Assign individual users to a Notification Team 48
7.3.2.2. Assign a Group of Users to a Notification Team 49
7.3.3. Removing users or groups from a notification team 50
7.4. Drafting a notification form – 'Notification form page' 51
7.4.1. Uploading supporting documents 55
7.4.2. Bulk deletion of supporting documents 56
7.5. Notification audit trail events 57
8. Specific actions on notification forms 58
8.1. Print a notification 58
8.2. Creating a notification from a pre-notification submitted through eNotifications 58
8.3. Copy a Notification 59
8.4. Deleting a Notification 60
8.5. Withdrawing a Notification 61
9. Notification forms / information sheets – workflow 62
9.1. Status: 'Draft' 62
9.2. Status: 'Finalised' 62
9.3. Status: 'Signed' 62

9.4. Status: 'Validated' 62
10. Annexes 63
10.1. Annex 1. User Authorisation Matrix 63
10.1.1. Authorisation matrix for 'Access management' Module (Section 6) 63
10.1.1.1. 'Access management' Module / 'Legal entity' tab 64
10.1.1.2. 'Access management module' / 'Offices' tab 65
10.1.1.3. 'Access management module' / 'Groups' tab 66
10.1.1.4. 'Access management module' / 'Users' tab 67
10.1.2. Authorisation matrix for 'Notifications' Module (section 6) 68
10.1.2.1. Notifications list page 69
10.1.2.2. Notification page – 'Notification Team' tab 70
10.1.2.3. Notification page – 'Notification' tab 71
10.1.2.4. Notification page – 'Audit trail'- tab 72
10.2. Annex 2: Overview of the buttons available in eNotifications 73
10.2.1. Buttons in Access Management Module: overview 73
10.2.2. Buttons in Notifications Module: overview 74
10.2.3. Buttons in Notifications forms: overview 75
10.3. Annex 3. Key differences between SANI2 and eNotifications 77

2. DOCUMENT HISTORY

Version	Changes	Date
1.00	First version	07/09/2026
1.01	Changes in the layout	10/09/2026
1.02	• Added section **4.5 Contact points in your legal entity (Member State)** • Updated section **7.2.2 Creating a simplified notification**, clarifying that an Encoder may create a simplified notification only if they are assigned to the Notification Team responsible for the standard notification linked to the prior approved aid number. If the Encoder is not a member of that original Notification Team, they will not be able to create a simplified notification for the prior aid number. • Updated section **8.3 Copy a Notification**, clarifying that notifications that were created using a previous, old version of the notification form cannot be copied.	06/10/2026

3. INTRODUCTION

3.1. Purpose of eNotifications

The eNotifications platform has been developed to facilitate the electronic transmission of State aid notifications, as required by Regulation (EC) No 794/2004. It replaces the State Aid Notifications Interactive ('SANI2') system, which had to be phased out because of outdated technology. Like SANI2, eNotifications is a multilingual application that allows Member State users to use the system and the forms in their own language.

eNotifications combines two main functions:

- It allows authorised users to complete the relevant notification forms directly in electronic format;
- It enables the full validation and transmission process to take place within a single application.

3.2. Purpose and scope of this manual

This user manual explains how to use eNotifications to prepare, manage and submit notifications in the system. It describes each step of the user process, including how to request access, choose the correct user profile, create and complete a notification, sign and validate it, and, where relevant, withdraw it.

The manual also describes the main functions of the Access Management Module and the Notifications Module. These functions include managing Legal Entities, Offices, groups and users, as well as handling attachments, searches, printing and audit trails.

This manual is designed to help users perform their tasks according to their role and permissions. It does not replace the applicable legal framework, internal procedures or business rules governing notifications, which continue to apply in full.

3.3. URLs and contact points

- The eNotifications platform can be accessed, once a user account has been activated by an authorised person, via the following site: https://competition-notifications.service.ec.europa.eu.
- Support e-mail: COMP-ENOTIF-SA-SUPPORT@ec.europa.eu
- State aid legislation: https://competition-policy.ec.europa.eu/state-aid/legislation_en

4. GETTING ACCESS AND SUPPORT FOR ENOTIFICATIONS

4.1. Who grants access

Access to eNotifications is managed at national level. For national authorities, there are two user profiles involved in managing the tool and users:

- Central Administrator (mandatory)
- Local Administrator (optional – available for countries that opt to create Offices within their Legal Entity).

4.2. Access to eNotifications

To get access, users need to contact their Central Administrator or, where applicable, Local Administrator, who will create an account for them in eNotifications. They then need to provide the Central or Local Administrator with the following details:

- full name
- e-mail address of their EU Login account or for which they will create their EU Login account (an EU Login account with two-factor authentication enabled is mandatory);
- the Office to be assigned to, if necessary;
- required user profile(s) (User profiles and permissions).

4.3. Required EU Login account

EU Login is the European Commission's Single Sign On (SSO) user authentication service. It allows authorised users to access a wide range of Commission web services, using a single e-mail address and password. An EU login account with two-factor authentication is mandatory to access eNotifications.

For step-by-step instructions browse this official EU Login portal page.

4.4. Login, user profiles and homepage

The modules displayed after you log in to eNotifications depend on the profile you use to log in. To view the profile currently in use, check the area below your name. If you have more than one profile, you can switch profiles:

1. open the profile list from the drop-down arrow menu;
2. select the required profile.

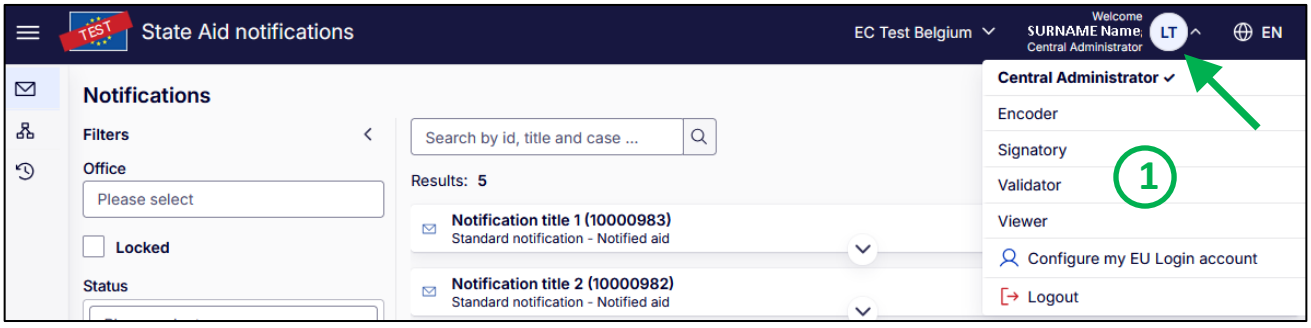


Figure 1: Switching user profiles

Administrative profiles, such as **Central Administrator** (point 1, Figure 2) or, where applicable, **Local Administrator**, can access both the **Access Management Module** and the **Notifications Module** (point 2, Figure 2).

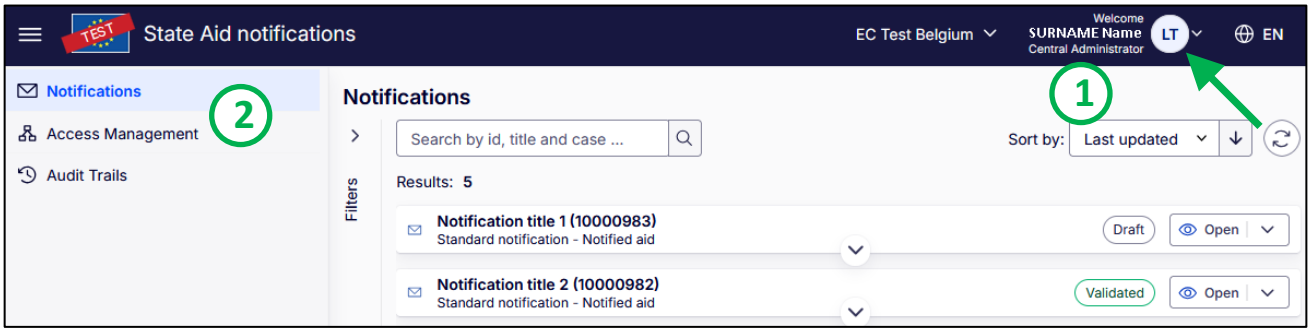


Figure 2: Central Administrator having access to both the notifications and access management

Notification related user profiles (e.g. Encoder, Signatory, Validator) can access only the **Notifications module**. eNotifications automatically saves the user's last-used settings, such as profile and language.

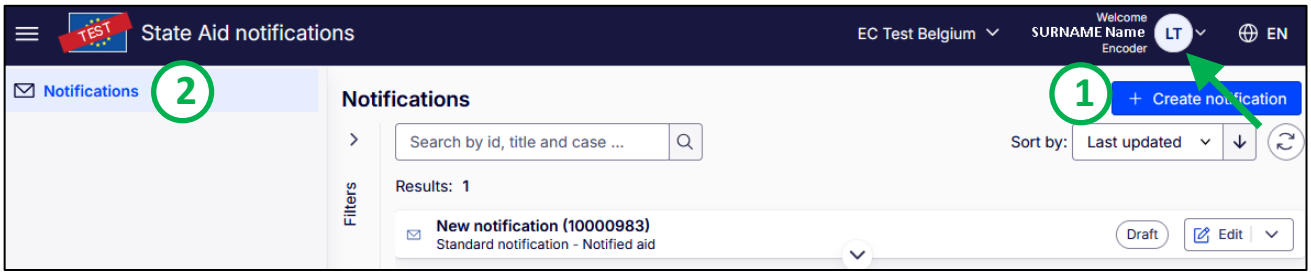


Figure 3: Notification workflow profiles having access only to the notification module

4.5. Contact points in your legal entity (Member State)

Via "My account details", in the menu accessible from the top-right of the screen, you can view your EU Login account details and information on how your account is used in the eNotifications system, for example your assignment to Offices and Groups. You can also consult the list of contact persons for your legal entity.

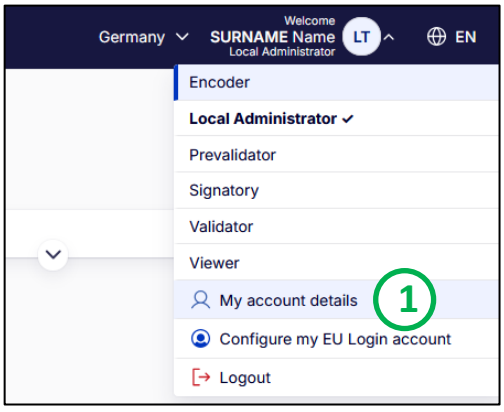


Figure 4: My account details

The contact persons for your legal entity can be consulted in the 'Contact persons'-tab (Figure 5, point 1). Central Administrators (Figure 5, point 2) are colleagues with the authority to manage all users within the legal entity.

Local Administrators (Figure 5, point 3) are colleagues responsible for users assigned to a specific Office. You will only see the Local Administrators for the Offices to which you are assigned.

For support and if you are assigned to an Office, you are advised to contact one of the Local Administrators first.

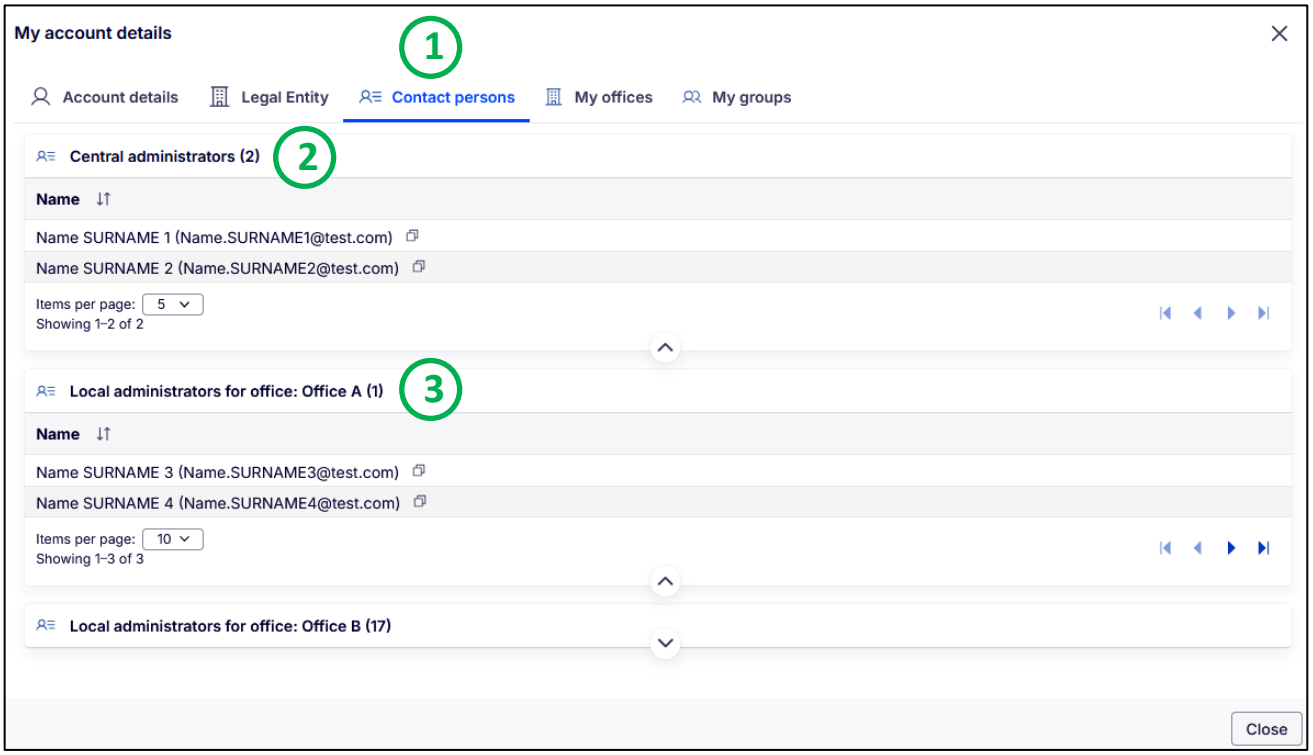


Figure 5: My account details - Contact persons

5. USER PROFILES AND PERMISSIONS

Users are anyone who requires access to eNotifications, either to manage other users - such as Central and Local Administrators - or to create and manage notification forms. A user may hold one or more profiles in eNotifications. The authorisation matrixes can be found in Annex 1. User Authorisation Matrix.

5.1. User profiles involved in access management

There are two profiles responsible for managing Users, Offices and Groups in eNotifications.

5.1.1. Central Administrators

At national level (Legal Entity), Central Administrators serve as the main contact point for eNotifications in their country. They oversee the full organisational structure of their Member State within eNotifications. Their responsibilities include creating and managing users throughout the country, as well as creating Offices when necessary. Since their role applies to the entire national structure, Central Administrators cannot be linked to a specific Office. Each Member State must appoint at least one Central Administrator.

5.1.2. Local Administrators

If Offices have been established, Central Administrators may transfer responsibility for Office-level user management to Local Administrators assigned to those Offices. Local Administrators are responsible for

managing users and groups within their own Office. Each Office should have at least one Local Administrator. If an Office does not have a Local Administrator, responsibility for user and group management remains with the Central Administrator(s). Where no Office has been created under the Legal Entity, the Local Administrator profile cannot be assigned to any user.

These two profiles cannot be assigned to the same user, as this would be redundant. A Central Administrator already has the ability to manage all offices within the Legal Entity.

Both Central and Local Administrators are responsible for:

- creating and managing additional Administrators for their Member State and Offices;
- managing all users involved in handling the notifications described below for their Member State and subordinate Offices;
- reassigning notifications within the limits of their respective responsibilities.

Central Administrators and Local Administrators have access to audit trail information for the full scope of their Member State.

Central Administrators may withdraw notifications for their Member State, while Local Administrators may withdraw notifications for their own Office.

An overview of all access rights can be found in Annex 1. User Authorisation Matrix.

5.2. User profiles involved in submitting notification forms

The notification workflow includes the following user profiles: **Encoder, Signatory, *Pre-validator,* Validator** and, where applicable, **Viewer.** The ***Pre-validator*** profile is available only to Member States that have chosen to include a pre-validation step in their workflow.

Only users who are 1) assigned to the notification team and 2) hold the required notification workflow profile can access a notification form and perform the actions linked to that profile. In practice, this means that a profile on its own does not grant access or permissions for a specific notification. The user must also be explicitly added to that notification team. As a result, before a notification can progress from e.g. Draft to Finalised, or move to any next step in the workflow, the notification team must include at least one user with the profile required for that next step. If no such user is assigned, the notification cannot advance. See also section Authorisation matrix for 'Notifications' Module (Section 6).

5.2.1. Encoder

Encoders can:

- create draft notifications;
- As a member of the notification team, Encoders can:
  - update draft notifications;
  - finalise draft notifications;
  - manage the notification team;
  - delete the notification;
  - create a notification from a pre-notification;
  - copy a notification to a new notification.

5.2.2. Signatory

As a member of the notification team, Signatories can:

- update finalised notifications, if necessary;
- sign finalised notifications (the electronic signature in the system is equivalent to a handwritten signature; once signed, subsequent actors in the workflow can no longer edit the notification); or;
- refuse to sign (reject) and send the notification back to the Encoder with a comment explaining the reason for the refusal.
- manage the notification team.

5.2.3. Pre-validator

Pre-validation is an additional step in the notification workflow used only by those Member States that have specifically requested it from the Commission. It applies only to simplified and standard notifications, including pre-notifications and notifications for legal certainty, which have a non-agriculture- or fisheries specific objective. The Pre-validator profile is therefore available only to those Member States that use this step.

As a member of the notification team, Pre-validators can:

- pre-validate signed notifications and send them to the Validator; or
- reject pre-validation and send the notification back to the Encoder with a comment (in the event of rejection, the Pre-validator must provide comments explaining the reason for the refusal).
- A Pre-validator can also manage the notification team.

5.2.4. Validator

As a member of the notification team, Validators can:

- validate signed notifications and send them to the Commission; or
- reject validation and send the notification back to the Encoder (in the event of rejection, the Validator must provide comments explaining the reason for the refusal).
- withdraw notifications that have been validated and submitted to the Commission.
- manage the notification team.

5.2.5. Viewer

If a member of the notification team, a Viewer has read-only access to notifications for which they have been added to the notification team. This profile is intended for users who need to consult notification forms at any stage of the workflow without being able to edit them.

6. THE ACCESS MANAGEMENT MODULE

Each Member State is represented in eNotifications as a Legal Entity. This is the default organisational level of the system and the basis on which users, roles and notifications are managed. Where needed, Member States may also create Offices within that Legal Entity to delegate user management and/or separate notification-related activities according to their national administrative structure. The use of Offices is entirely optional: a Member State may operate solely at Legal Entity level or organise its work through one or more Offices. In this structure, Central Administrators manage the Legal Entity as a whole, including the creation of Offices and the management of users at national level, while Local Administrators manage users within the Offices to which

they are assigned. Since eNotifications does not impose any fixed hierarchy for Offices, each Member State can organise itself in the way that best reflects its institutional arrangements.

- Point 1, Figure 6: access to the access management module;
- Point 2, Figure 6: tabs to access and manage the legal entity, offices, groups and users.

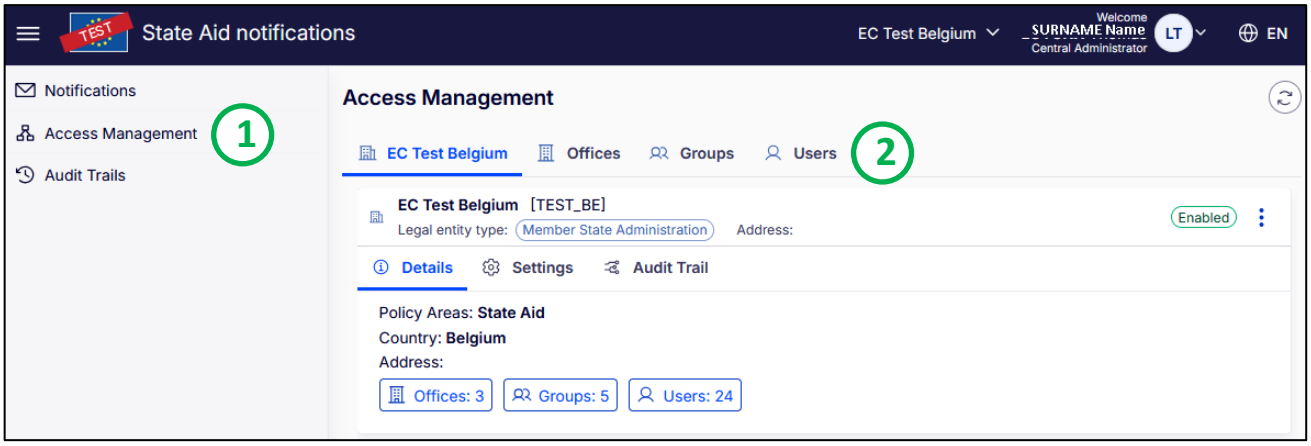


Figure 6: User access management module

6.1. Managing the Member State (Legal Entity)

Each Member State is represented in eNotifications as a Legal Entity. This is the main organisational level of the system and the basis on which users, roles and notifications are managed. Member States may operate only at Legal Entity level or create Offices within it, depending on their administrative organisation. Central Administrators manage the Legal Entity as a whole and cannot be assigned to an Office.

6.1.1. Editing Legal Entity 'Details'

Only Central Administrators can update the Legal Entity details. Select the 'Legal Entity'-tab (point 1, Figure 7), click the three dotted menu and select 'Edit' (point 2, Figure 7).

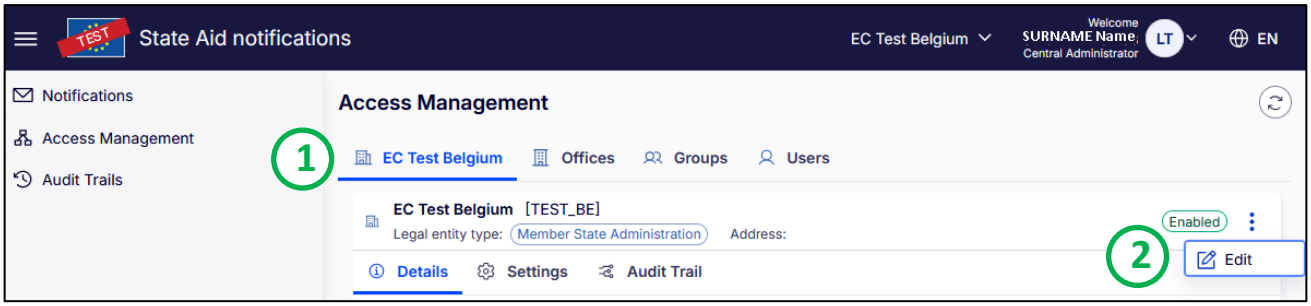


Figure 7: Edit the Legal Entity details

Amongst other data, it is possible to update the name and address (Figure 8). This information is purely informative. It is not used in or for the processing of the notifications.

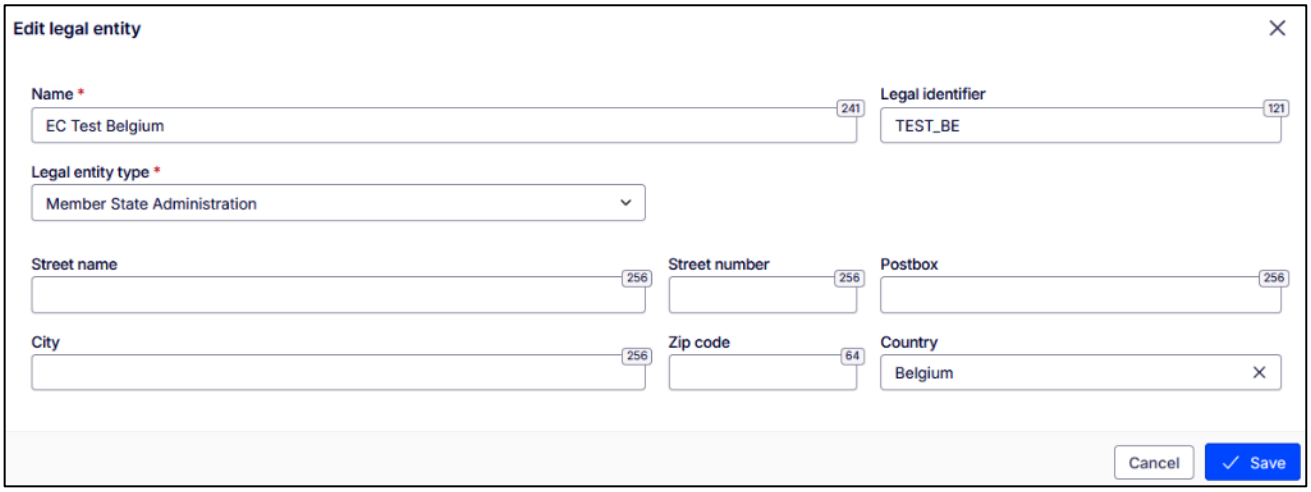


Figure 8: Legal Entity details

6.1.2. Setting for default read-only access for Central and Local Administrators

Under **Legal Entity** > **Settings** (point 1, Figure 9), Central Administrators can consult whether Central and Local Administrators are granted read-only access to notifications (point 2, Figure 9) **without the need to be assigned to the notification team**.

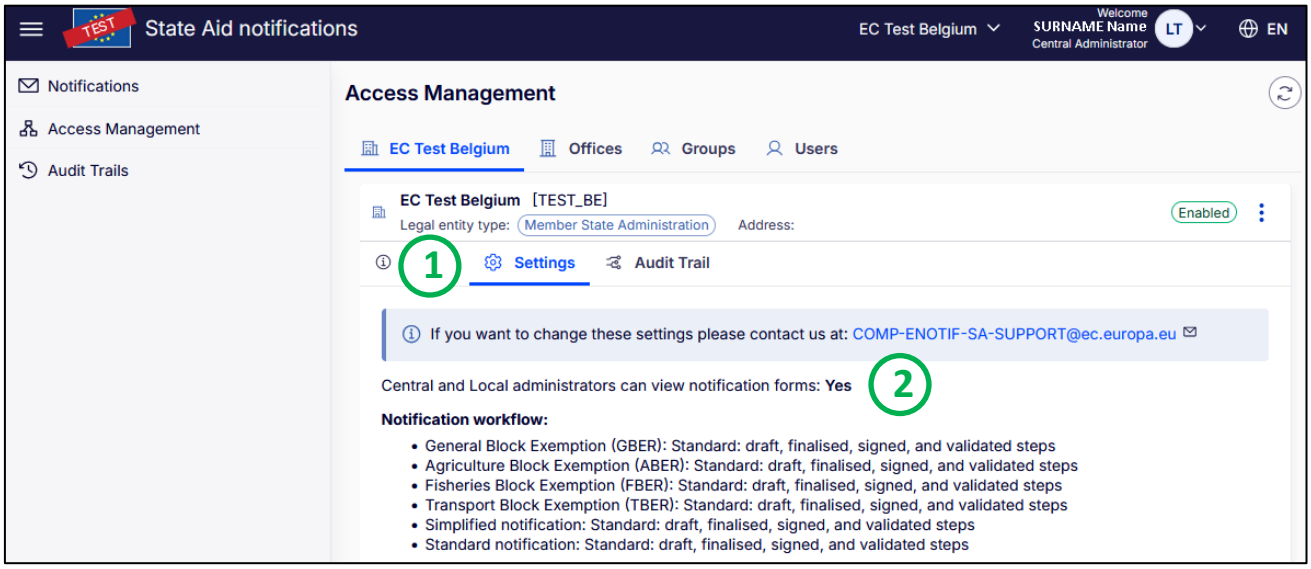


Figure 9: Setting for default read-only notification access for Central and Local Administrators

6.1.2.1. Default read-only notification access is enabled

When this setting is enabled, Central Administrators and, where applicable, Local Administrators are by default granted read-only access to the content of notifications, including attachments and comments, without the need of being a member of the relevant notification team.

More specifically:

- **Central Administrators** have read-only access to the details of **all** notifications within the Legal Entity;
- **Local Administrators** have read-only access to the details of **all** notifications **belonging to their Office(s)**.

As a result, within their respective scope:

- The 'notification form'-tab is visible (point 1, Figure 10) providing read-only access to all form sections, attachments and comments (point 2, Figure 10). An informative message explains that the notification is in read-only mode for the Administrator (point 3, Figure 10).
- print notification content without being part of the notification team (point 4, Figure 10).

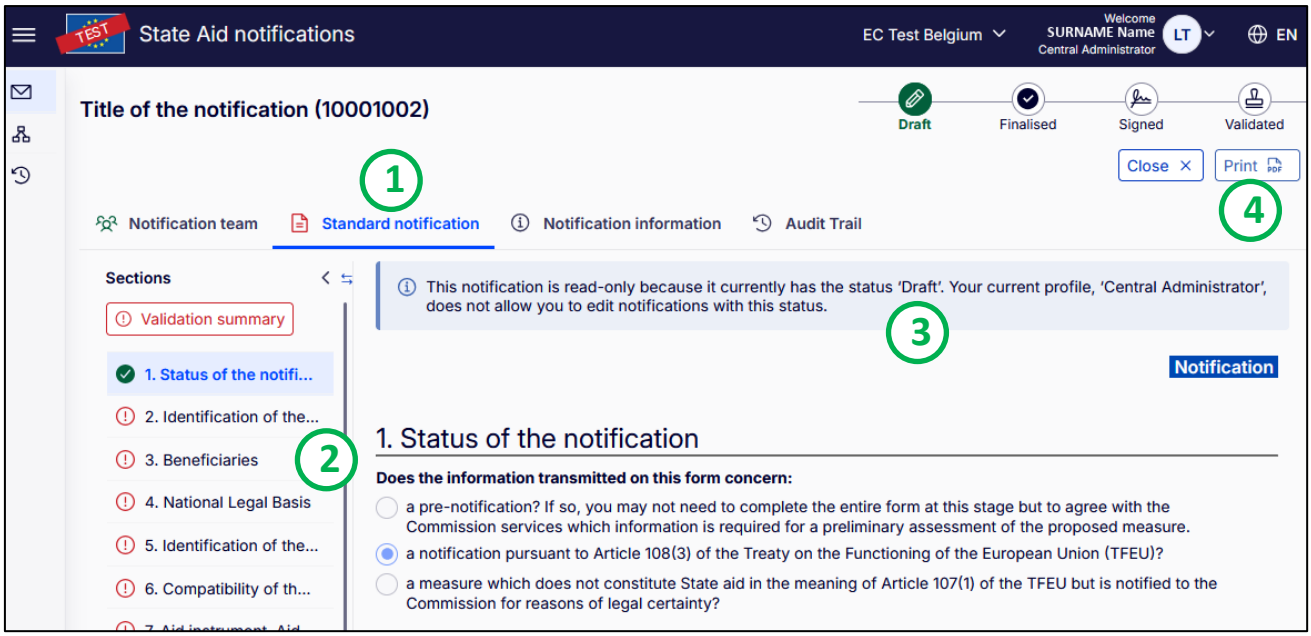


Figure 10: Default read-only notification access enabled for Central and Local Administrators

In line with the access rights available in SANI2, this setting is enabled by default in eNotifications. However, granting Central and Local Administrators read-only access to all notification details and attachments may entail a security risk if their accounts are compromised. The decision and responsibility for keeping this setting enabled rests with the Member State.

To update this setting, please contact COMP-ENOTIF-SA-SUPPORT@ec.europa.eu. For security reasons, Member States cannot change this setting themselves.

6.1.2.2. Default read-only notification access is disabled

When the setting is disabled, Central and Local Administrators do not have automatic read-only access to notification content for notifications to which they have not been assigned. The 'notification form' tab will not be available.

However, they can still (Figure 11):

- manage the notification team;
- access the notification summary;
- withdraw the notification (point 2, Figure 11).

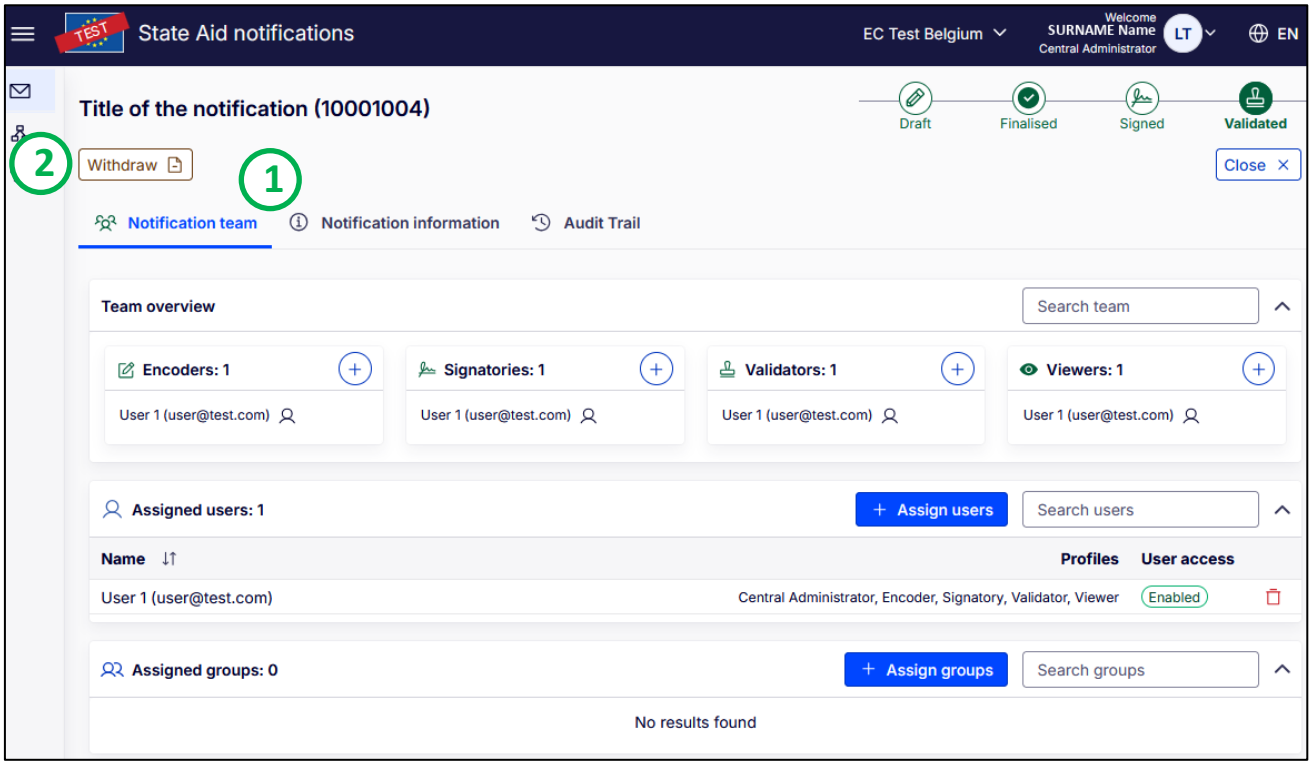


Figure 11: Default read-only notification access disabled for Central and Local Administrators

In such cases, users must be added to the relevant Notification Team in order to consult notification details and attachments and/or print the notification.

Please note that, to be assigned to a Notification Team, a user must have at least one notification workflow profile assigned, i.e.: Viewer, Encoder, Signatory, Pre-validator, or Validator (see Section 4.2.). Users who only have the Central Administrator or Local Administrator profile cannot be assigned to a Notification Team.

6.2. Office management

Member States may choose to organise their activities in eNotifications through Offices. The use of Offices is optional and depends on the institutional set-up and the way functions are organised within the Member State.

Offices serve two main purposes:

- to delegate user management to Local Administrators, in particular in large or decentralised Member States;
- to separate notification-related activities.

There is no hierarchy or fixed set of rules governing the creation of Offices. Offices may be created, for example, on a geographical basis (such as regions), by granting authority, or by sector, for instance to separate agriculture- and fisheries-related users and notifications. Through an Office it is thereby possible to create and submit notifications on behalf of an Office. In the system, notifications can be filtered based on the Office on behalf of which the notification was created and submitted (point 1, Figure 12).



Figure 12: Filter notifications on Office

6.2.1. Create an Office

Only Central Administrators can create new Offices. Each new Office should have at least one Local Administrator responsible for user management in that office; otherwise, the responsibility for the management of users and groups remains entirely with the Central Administrator(s). Central Administrators are responsible for managing the entire Legal Entity, including its Offices. As a result, they cannot be assigned to an Office.

If you are a Central Administrator (point 1, Figure 13), you can create a new Office from the 'Offices' tab (point 2, Figure 13). Next, click '**+ Create office**' (point 3, Figure 13). You will then be asked to provide the following information:

- **Office name** – **mandatory**. Choose the name carefully, as the Office is one of the criteria available for filtering. Offices cannot share the same name; the name must be unique.
- **Office description** – **optional**. A description of the Office that provides additional context, e.g. the purpose of the Office or a description of the type of users that are assigned to it.

Both fields can be edited later, if needed. Once you have entered the required information, click '**Save**'. The newly created office will then appear in the list of Offices.

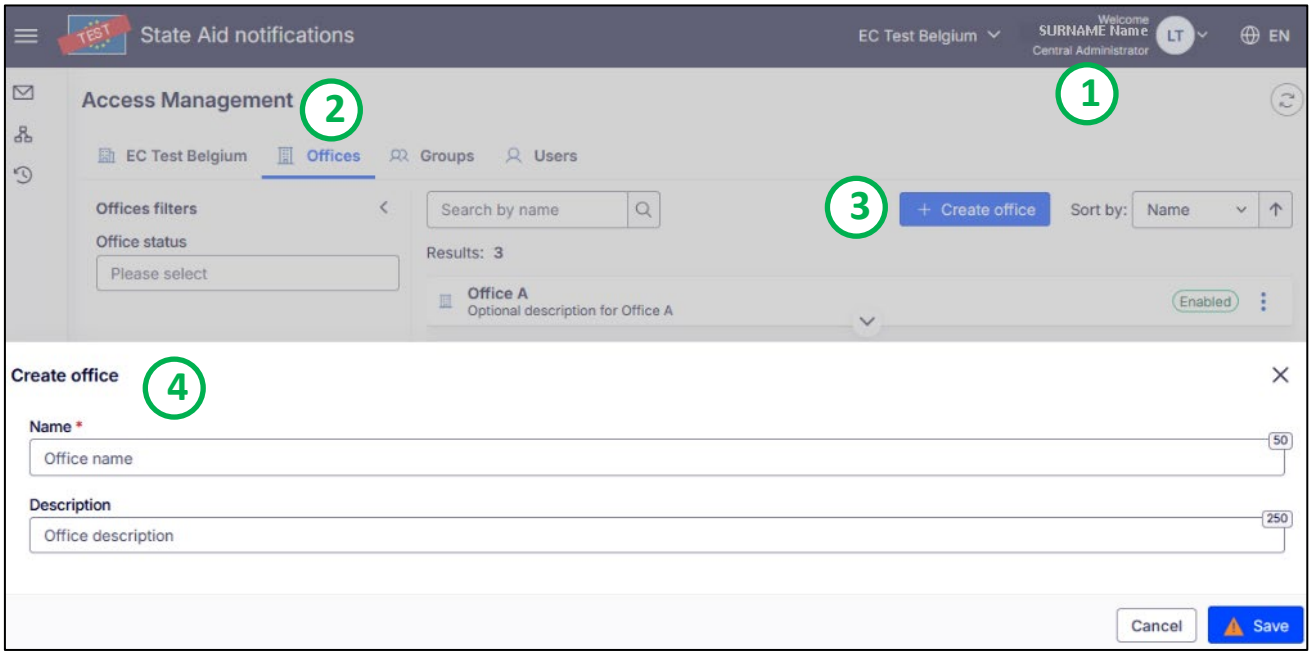


Figure 13: Create a new Office

6.2.2. Update an Office

It is possible to update the name, description an Office. The name of the Office must be **unique** within the Legal Entity (Member State). Click the three dotted menu (point 1, Figure 14) and click '**Edit**' (point 2, Figure 14).

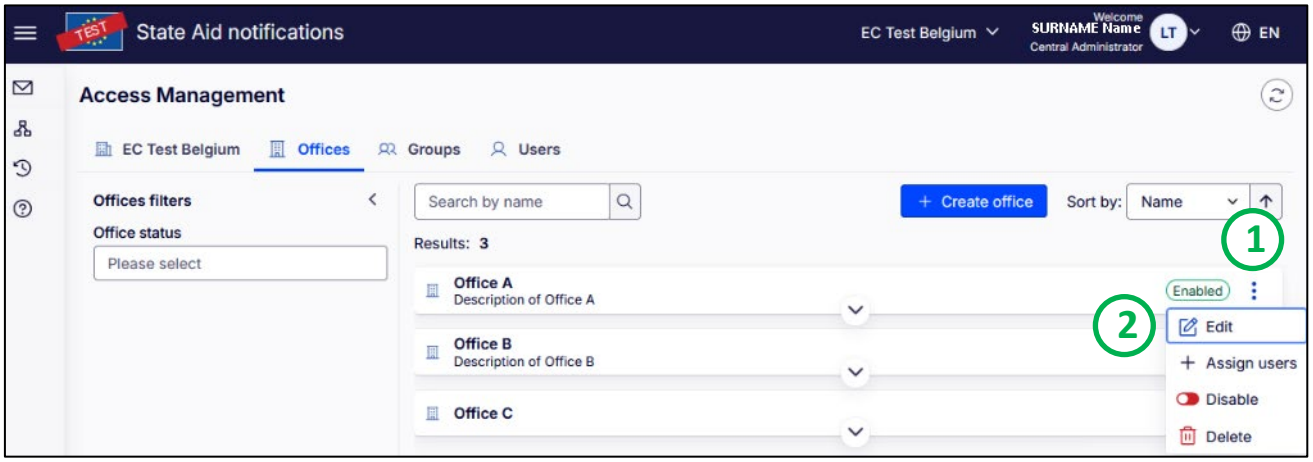


Figure 14: Update an Office

The 'Edit office'-window opens. Click the 'Save'-button to apply changes (Figure 15).

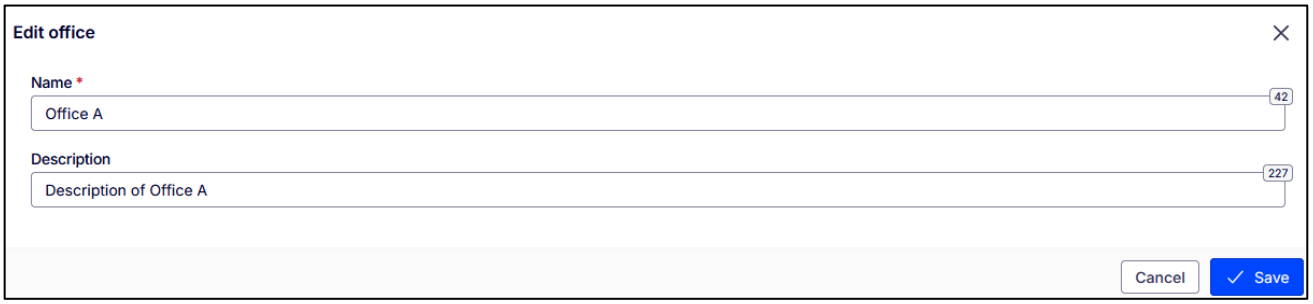


Figure 15: The 'Edit office'-window

6.2.3. Assign users to an Office

6.2.3.1. Assign users to an Office from the 'Offices'-tab

Users (incl. Local Administrators) can be assigned by first expanding the Office panel (point 1, Figure 16) and then clicking the '**+ Assign users**'-button (point 2, Figure 16).

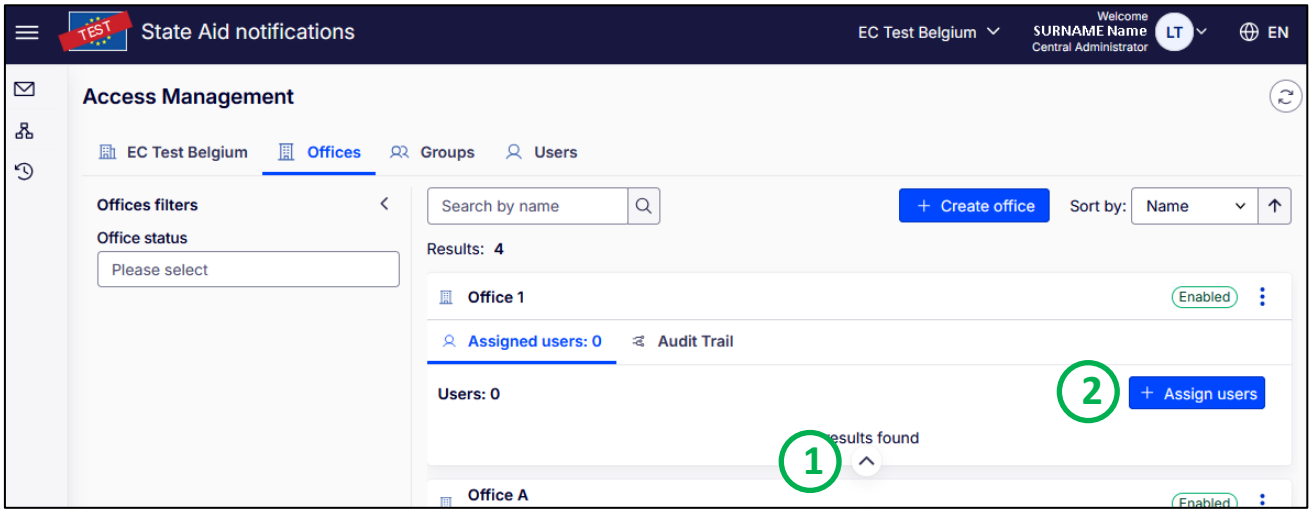


Figure 16: Assign users using the assign button in the expanded Office panel

or by first clicking the three dotted (⋮) menu button (point 1, Figure 17) and then click the '**+ Assign users**' option (point 2, Figure 17).

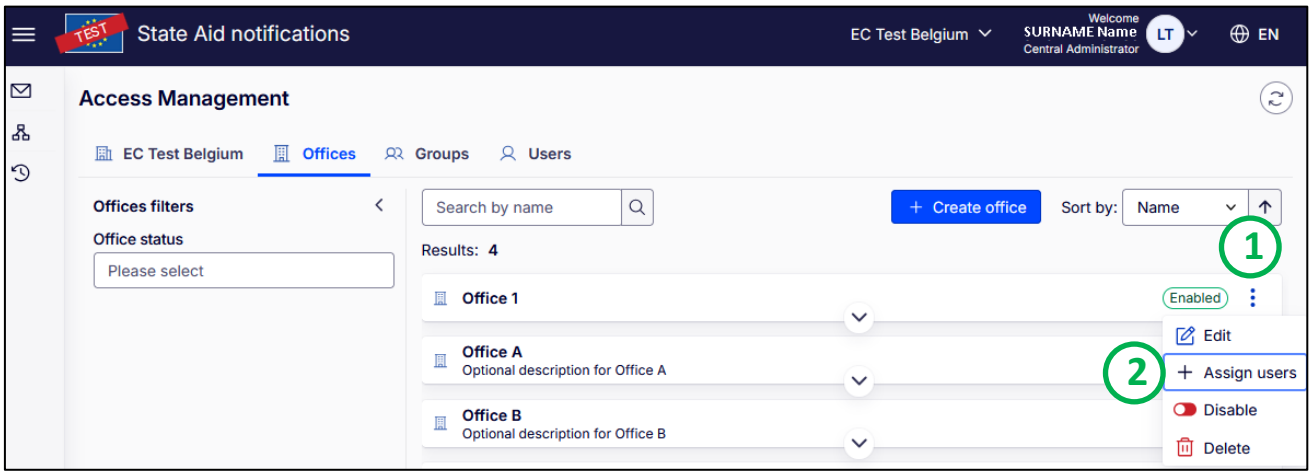


Figure 17: Assign users to an Office using the assign button in the three dotted menu

Through both options, the same 'Assign users to office'-window opens. It is possible to filter the searchable users based on their profile (point 1, Figure 18) and/or search for users by name, email or profile by using the corresponding search field (point 2, Figure 18).

You can search and add one or multiple users (point 3, Figure 18) before clicking the '**Assign**'-button to confirm (point 4, Figure 18).

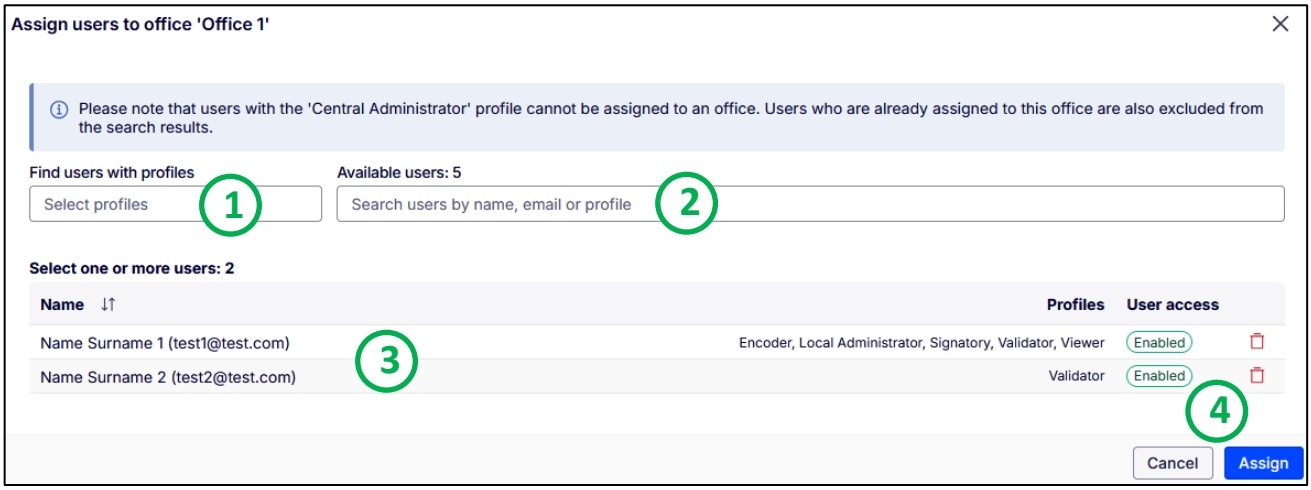


Figure 18: 'Assign users to an office'-window

6.2.3.2. Assign user to an Office from the 'Users'-tab

A user can also be assigned to an Office from the user's perspective. Navigate to the 'Users'-tab in the access management module and search for the user that needs to be assigned to an Office to start. Once you have found the user, there are two options to assign the user to the Office. The first option is by expanding the 'Users details'-panel (point 1, Figure 19). If the user has a Local Administrator profile but is not assigned to an Office, the system will show an informative message stating that without the assignment to an Office, the user cannot execute his role as Local Administrator (point 2, Figure 19). Click the '+ Assign offices' to open the 'Assign user to offices'-window (Figure 20).

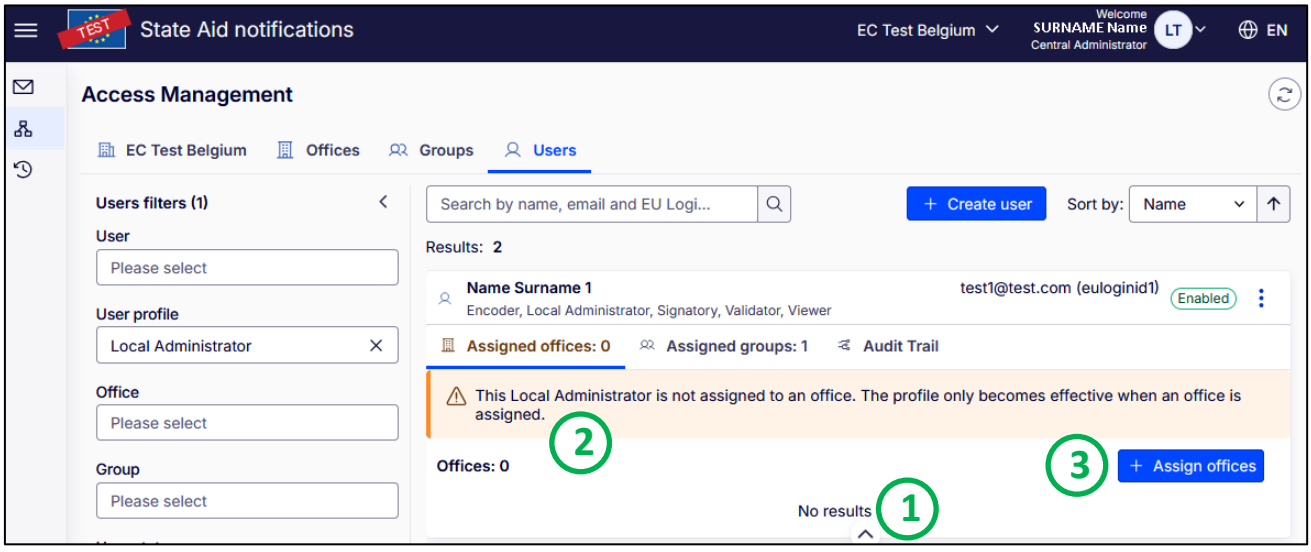


Figure 19: Assign user to an office from the expanded 'Assigned offices'-panel

Search an Office by its name or description and select one or more offices before clicking the 'Assign'-button to confirm (Figure 20).

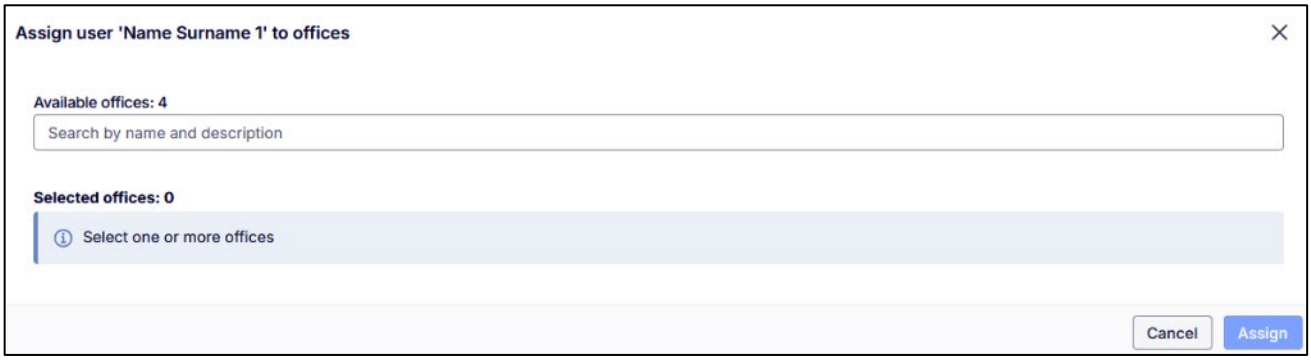


Figure 20: Select office(s) to be assigned to the user

The second approach is by clicking the three dotted (⋮) menu next to the right of the user's information (point 1, Figure 21) and select 'Edit' (point 2, Figure 21).

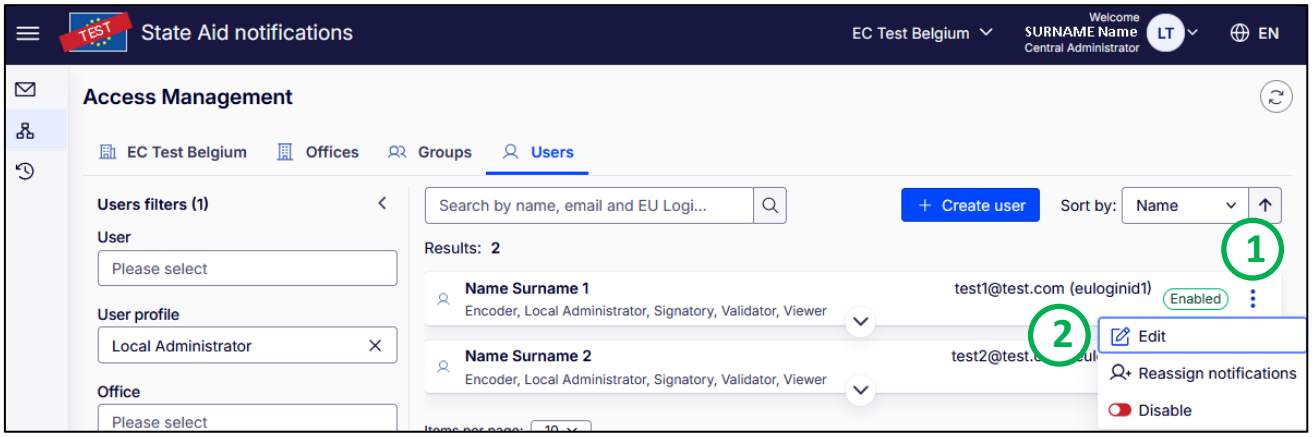


Figure 21: Assign user to an office by updating the user details

The 'Edit user details'-windows open that allows you to search and select one or multiple Offices to which the user needs to be assigned (Figure 22). **The Local Administrator profile cannot be assigned if no Office exists.**

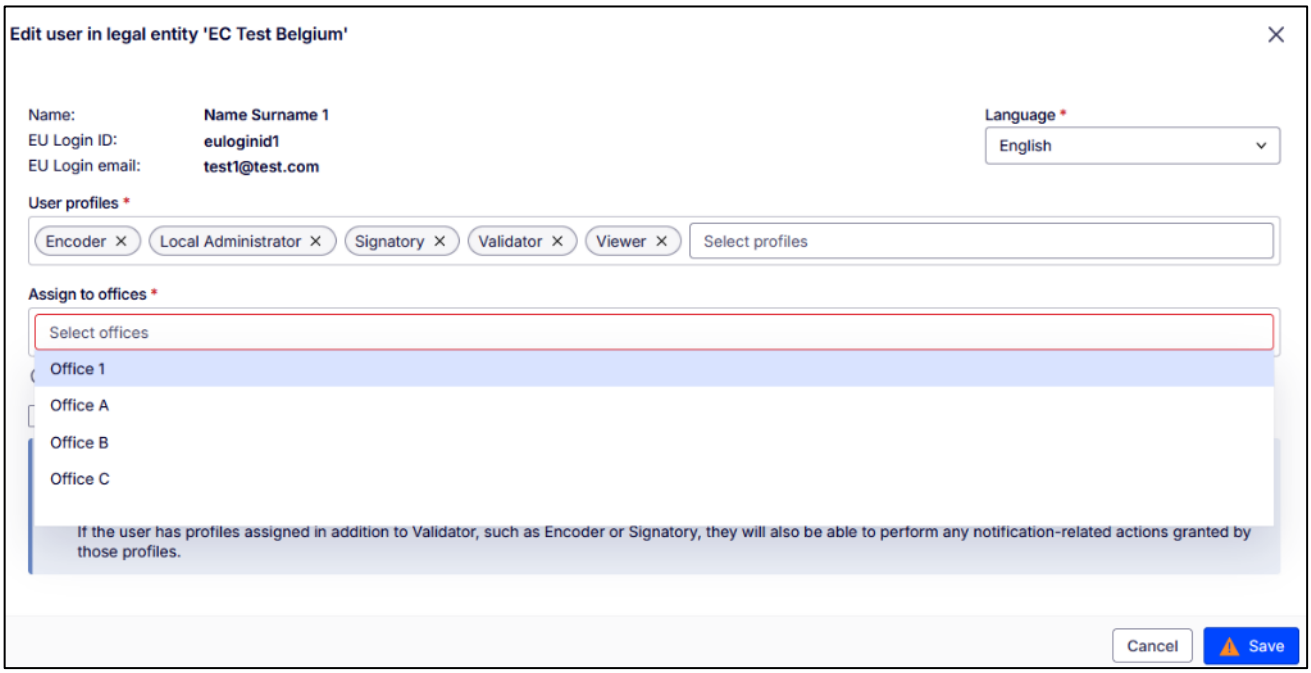


Figure 22: Edit user - assign (an) Office(s)

6.2.4. Remove users from an Office

Removing a user from an Office has mainly a purely organisational consequence that does not impact the user's permissions. The exception is if the user has the Encoder profile. As an Encoder, the user will no longer be able to create notifications on behalf of the Office.

Click the garbage bin icon to remove the user from the Office (point 1, Figure 23)

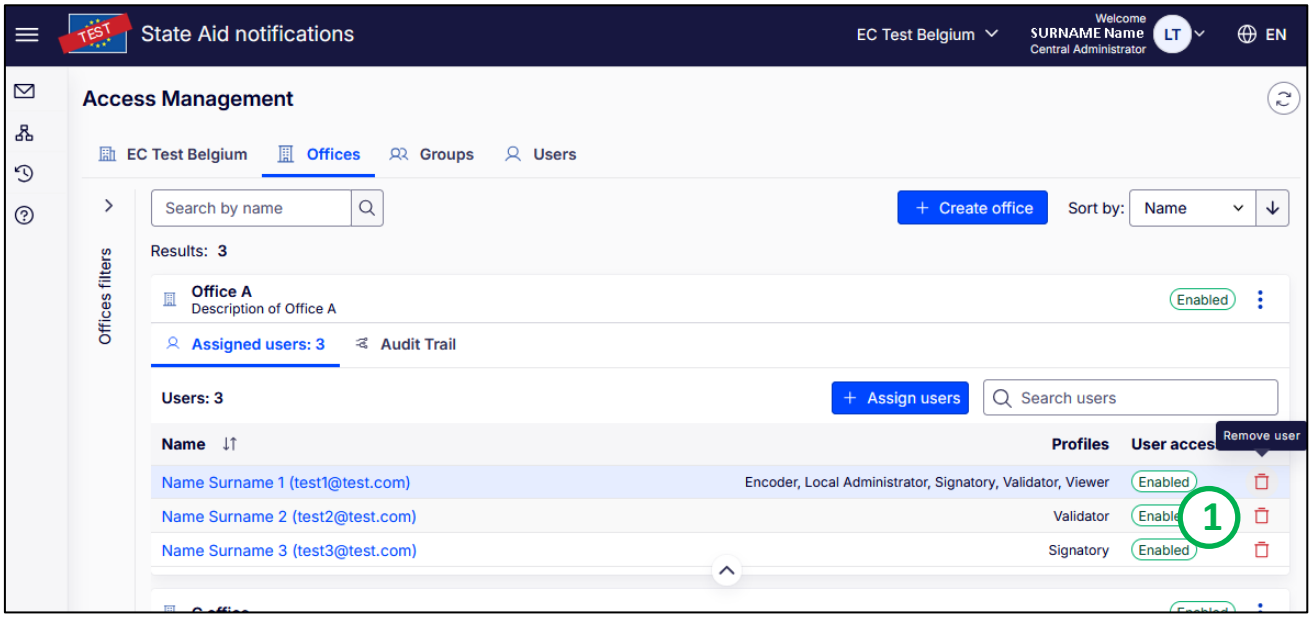


Figure 23: Remove a user from the Office

Click the 'Remove'-button to confirm the deletion (Figure 24).



Figure 24: Remove a user from the Office - Confirmation message

6.2.5. Disable or enable an Office

6.2.5.1. Disable an Office

When you disable an Office, the main consequence is that notifications can no longer be created on behalf of that Office. In this case, notifications created by Encoders assigned to the disabled Office and not being assigned to another Office, are created on behalf of the Legal Entity (Member State) instead.

A disabled Office does not impact the users and Groups assigned to that Office nor the notifications that were created by Encoders on behalf of the Office. The users and Groups assigned to the Office will remain active / enabled and they will retain access to the notifications, if assigned to the notification team. The Users and Groups of the Office will continue to operate on behalf of the Legal Entity (Member State) unless they are assigned to another Office.

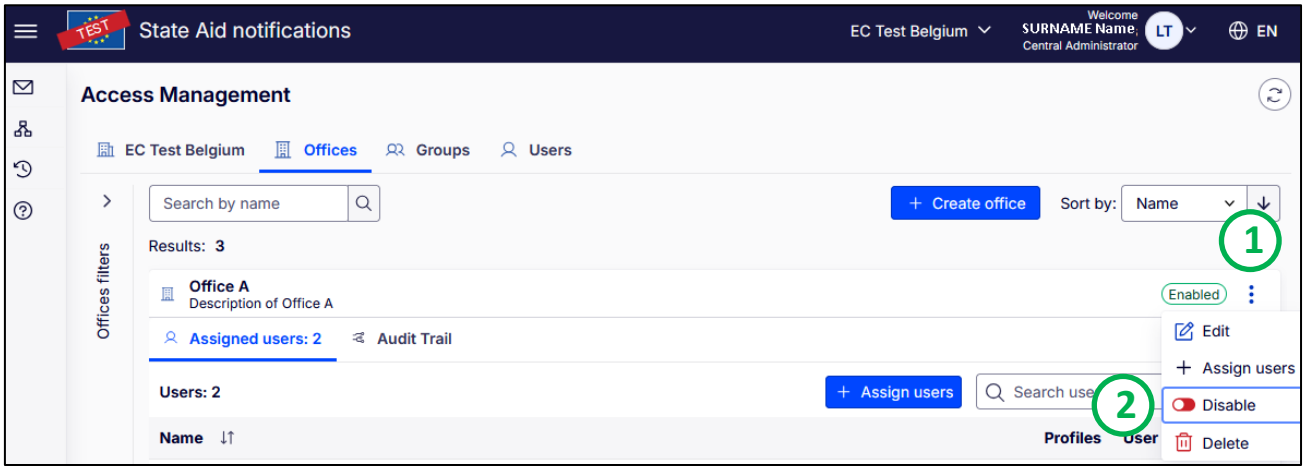


Figure 25: Disable an Office

Provide the reason for disabling the Office and click the 'Yes'-button to confirm.

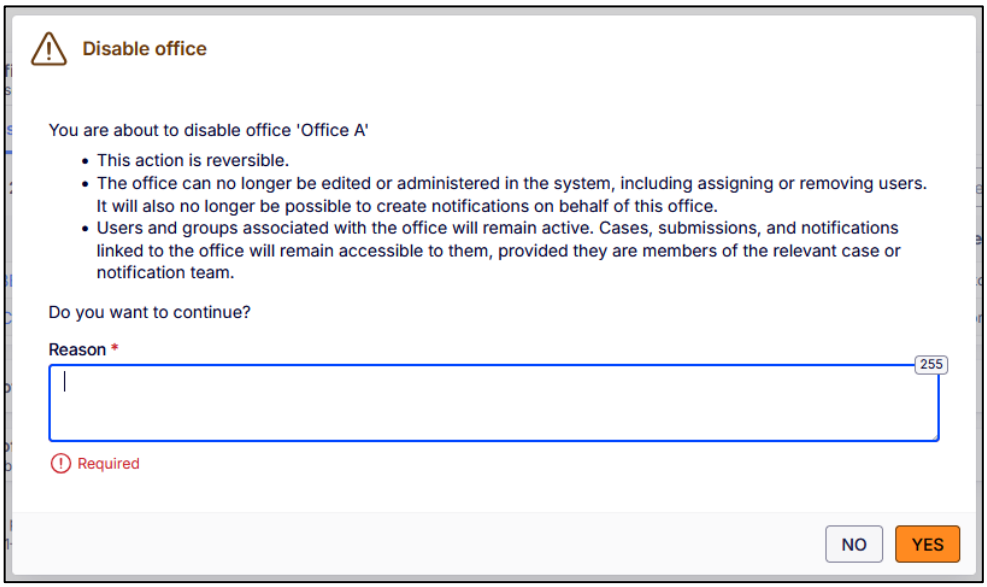


Figure 26: Disable an Office - Confirmation message

6.2.5.2. Enable an Office

When an Office is enabled, the assigned Users can operate again on behalf of the Office. This is mostly relevant for Encoders that can create notifications on behalf of the Office again.

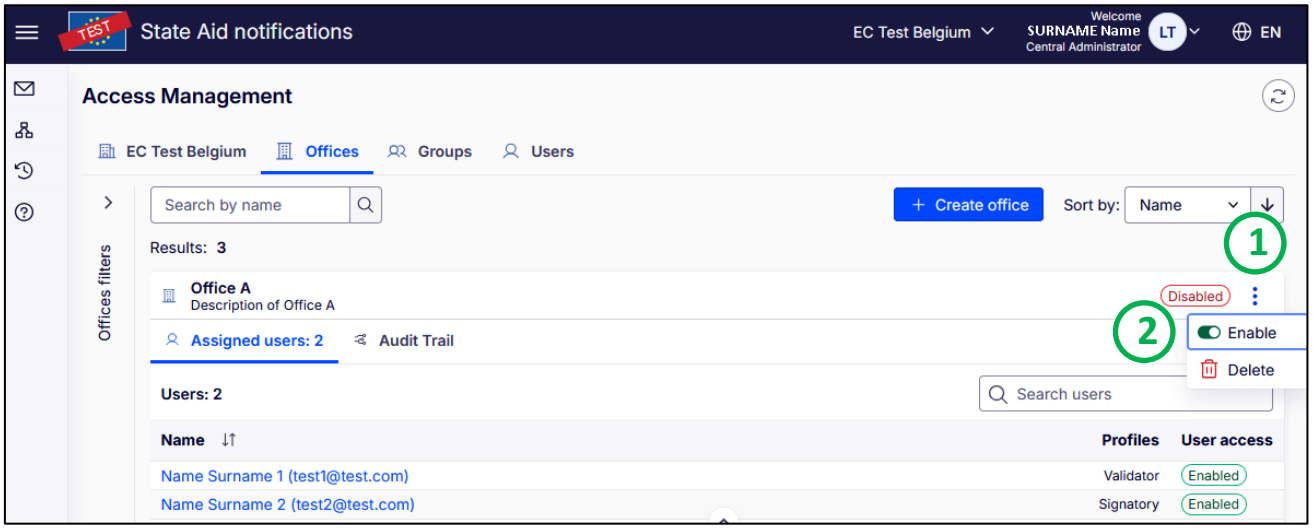


Figure 27: Enable an Office

Provide the reason for enabling the Office and click the 'Yes'-button to confirm (Figure 28).

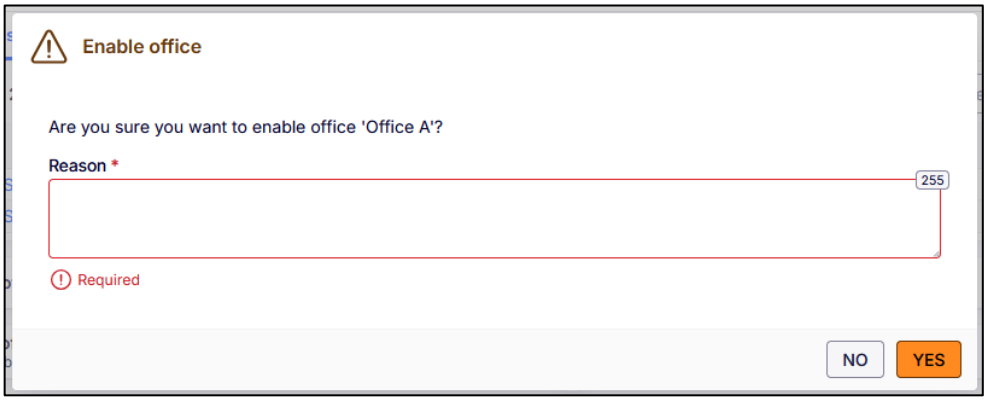


Figure 28: Enable an Office - Confirmation message

6.3. Group management

A group is a set of users. There are no restrictions regarding user type or Office affiliation when creating a group. Central Administrators can create groups at Member State level or for a specific Office, while Local Administrators can create groups for their own Office. The purpose of groups is to assign collaborative users to a notification team in a single step rather than searching and assigning each user to the notification team individually.

For this purpose, the group should include only users who collectively cover all required notification workflow profiles (i.e., Encoder, Signatory, (pre-validator) and Validator). This ensures that, once the group is added to a notification team, the notification can be handled throughout the entire workflow.

6.3.1. Create a Group

Groups are created in a similar way to Offices. To create a new Group, a Central or Local Administrator (point 1, Figure 29) clicks on the **'Groups'**-tab (point 2, Figure 29) and then selects **'+ Create group'** (point 3, Figure 29). The 'Create group'-window opens.

If a Central Administrator creates the Group, it can be assigned to an Office. If the Office has a Local Administrator assigned, that Local Administrator will also be able to manage the Group. A Group can be

assigned to only one Office at a time. If a Group is not assigned to an Office, it must be managed by the Central Administrator(s).

Local Administrators can create Groups at the level of their own Office. If a Local Administrator belongs to one Office only, the group will be assigned to that Office by default.

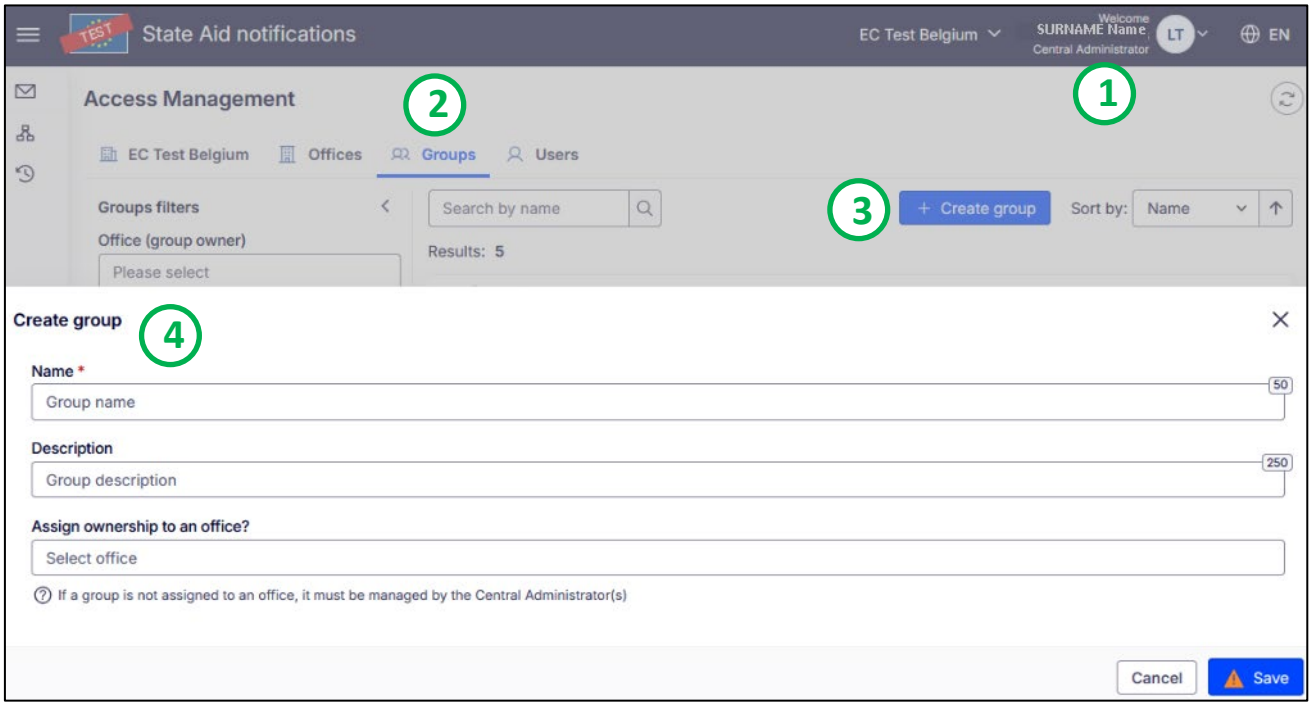


Figure 29: Create a new Group

6.3.2. Update a Group

It is possible to update the name, description and Office assignment (optional) of a Group. The name of the Group must be **unique** within the Legal Entity (Member State). Click the three-dotted (⋮) menu (point 1, Figure 30) and click 'Edit' (point 2, Figure 30).

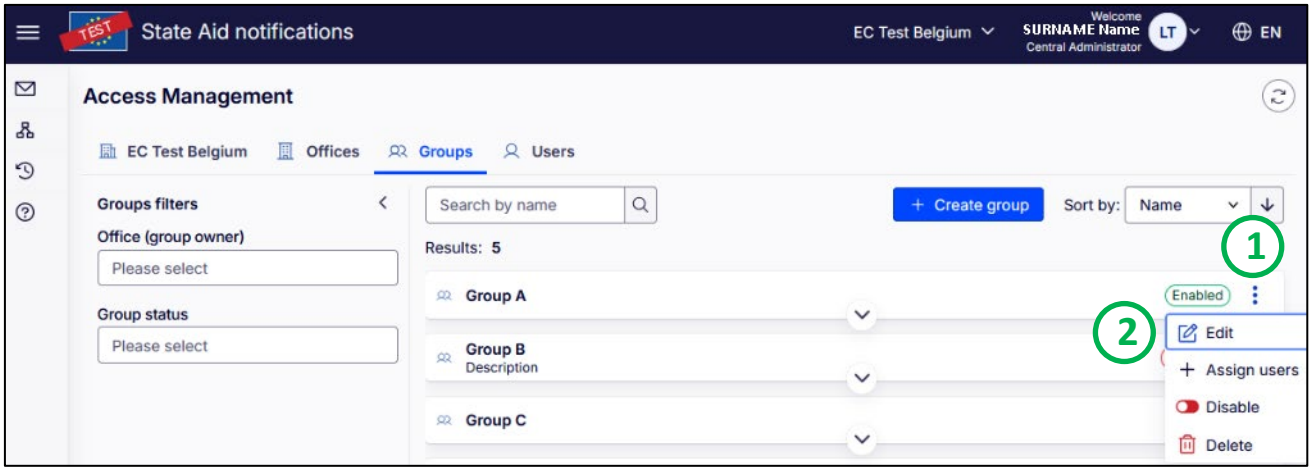


Figure 30: Update a Group

The 'Edit group'-window opens. Click the 'Save'-button to apply changes (Figure 31).

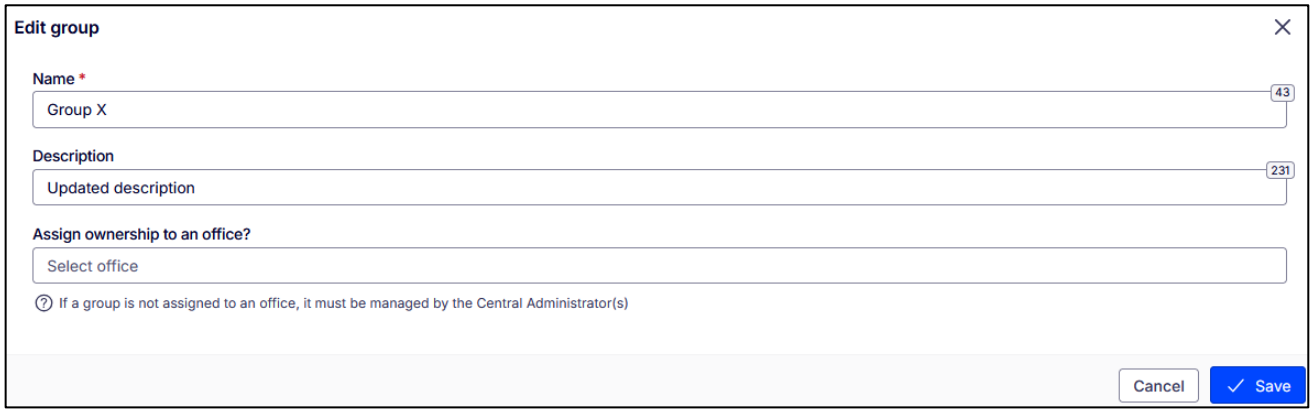


Figure 31: The 'Edit group'-window

6.3.3. Assign users to a Group

6.3.3.1. Assign users to a Group from the 'Groups'-tab

Users (incl. Local Administrators) can be assigned by first expanding the Group panel (point 1, Figure 32) and then clicking the '+ Assign users'-button (point 2, Figure 32)

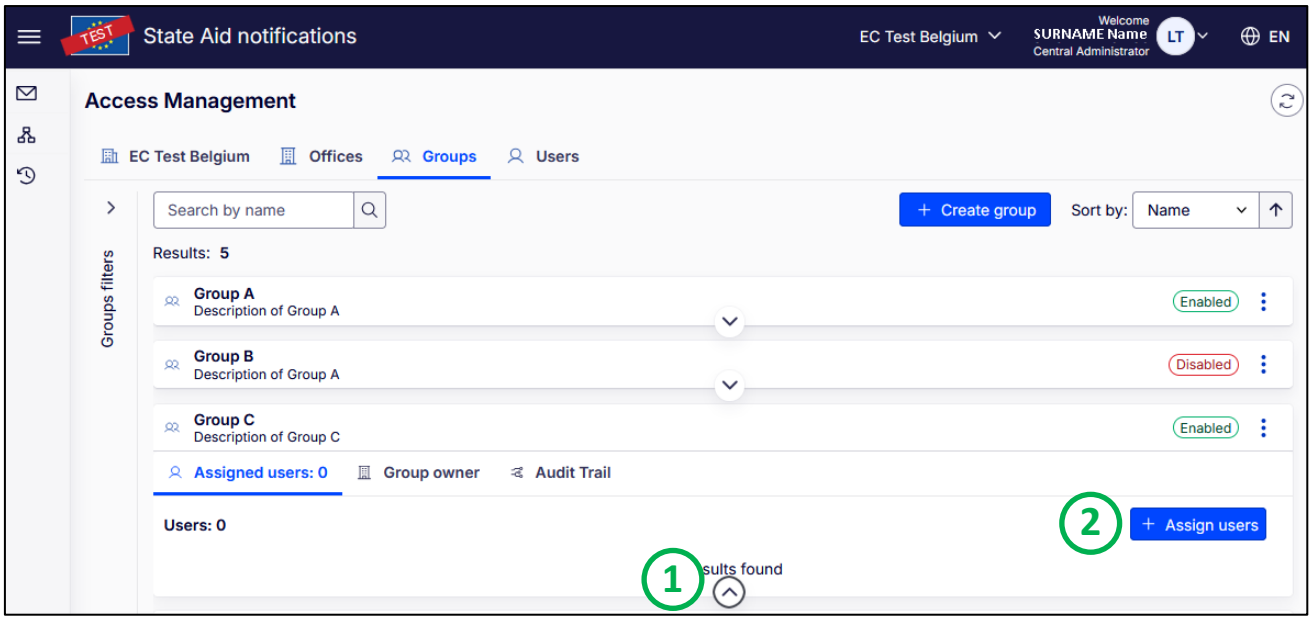


Figure 32: Assign users using the assign button in the expanded Group panel

or by first clicking the three dotted menu button (point 1, Figure 33) and then click the '+ Assign users' option (point 2, Figure 33).

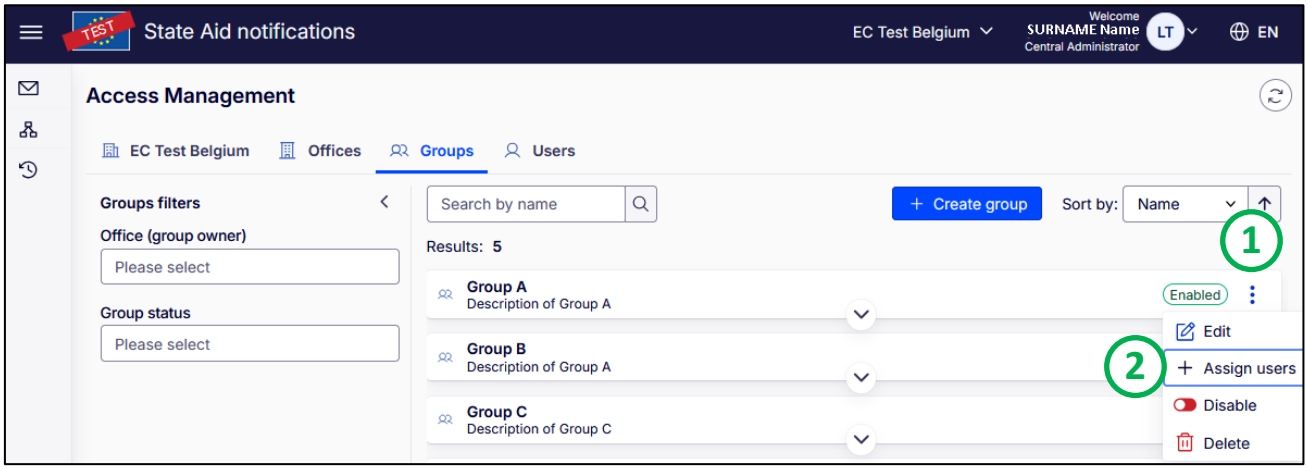


Figure 33: Assign users to a Group using the assign button in the three dotted menu

6.3.3.2. Assign user to a Group from the 'Users'-tab

A user can also be assigned to a Group from the user's perspective. Navigate to the 'Users'-tab in the access management module and search for the user that needs to be assigned to a Group to start. Once you have found the user expand the 'Users details'-panel (point 1, Figure 34). Select the 'Assigned groups'-tab (point 2, Figure 34) and click the '**+ Assign offices**'-button (point 3, Figure 34) to open the 'Assign user to groups'-window (Figure 35).

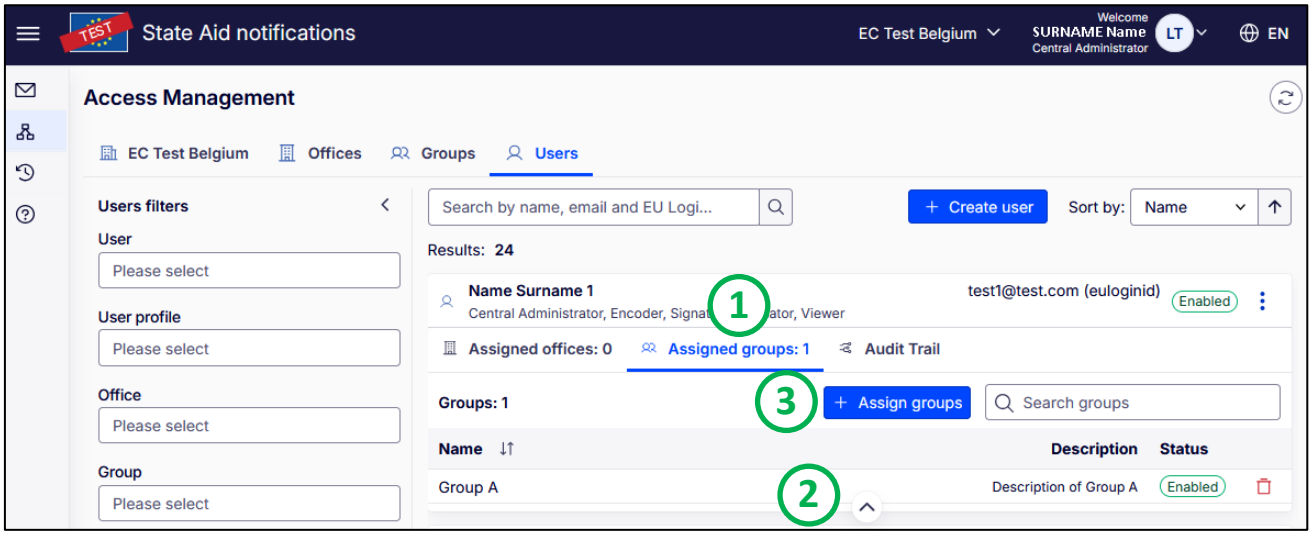


Figure 34: Assign user to a group from the expanded 'Assigned groups'-panel

Search a Group by its name or description and select one or more groups before clicking the 'Assign'-button to confirm (Figure 35).



Figure 35: Select group(s) to be assigned to the user

6.3.4. Remove users from a Group

Removing a user from a Group does not affect the user's permission to access the system. However, the user will no longer have access to notifications to which the Group was assigned. Navigate to the Group in the 'Groups'-tab (point 1, Figure 36) and click the 'Garbage bin'-icon (point 2, Figure 36).

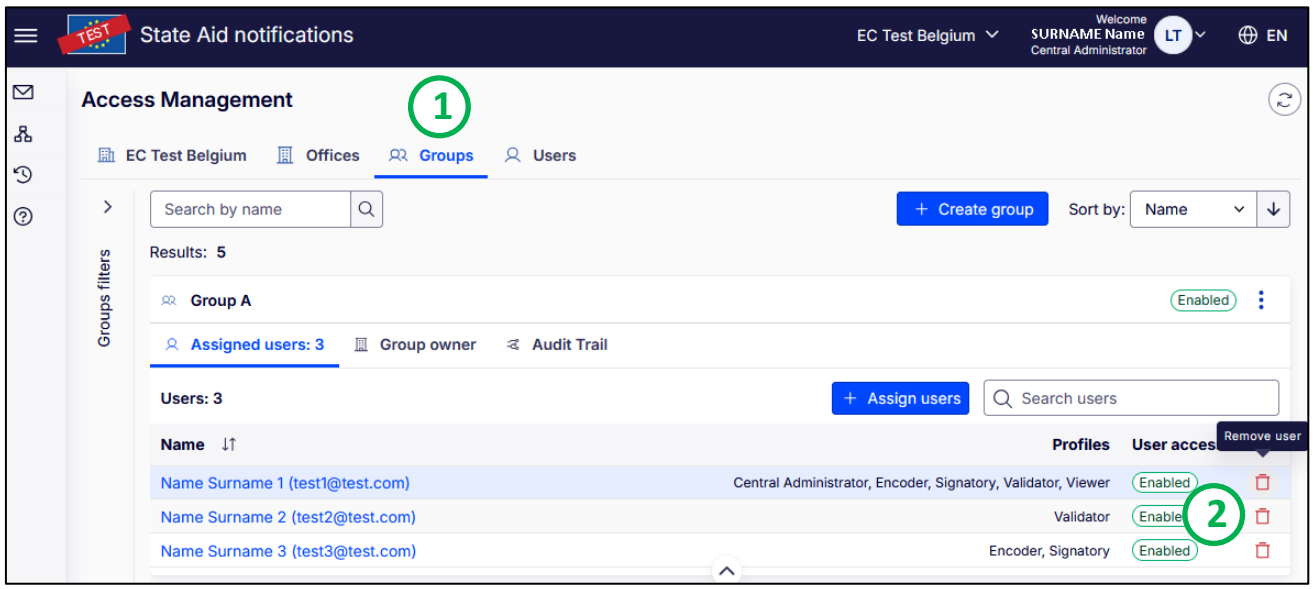


Figure 36: Remove a user from a Group

The 'Remove user'-window opens, requesting for confirmation and explaining the consequences of the action. Click 'Remove' to confirm.

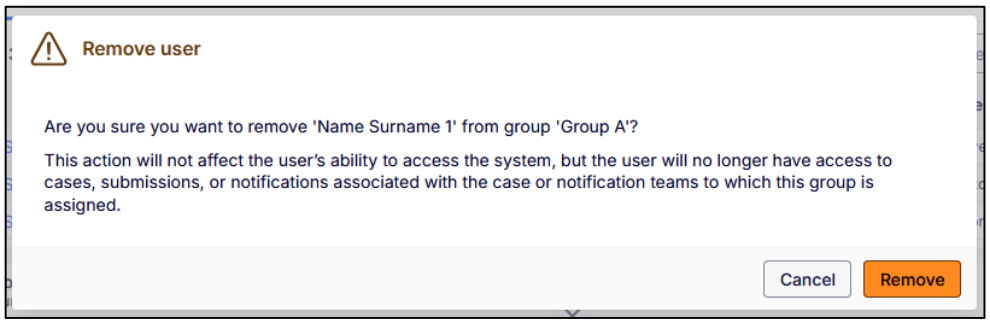


Figure 37: Remove user from a Group - Confirmation window

6.3.5. Disable or enable a Group

6.3.5.1. Disable a Group

When a Group is disabled, it is no longer possible to apply changes to the Group (incl. adding or removing users). In addition, the Group will no longer be able to be assigned to a Notification Team. However, disabling a Group does not revoke its users' access to existing notification assignments. The users of the Group will retain access and can continue to contribute to the notifications. So, if the goal is to revoke a Group's access to its notifications, the Group must be removed from the Notification Team (see Removing users or groups from a notification team).

Central Administrators can:

- create Offices and Groups at Member State and Office level;
- enable an Office or Group;
- disable an Office or Group;
- assign a Group to an Office;
- delete an Office or Group, provided that it has no users assigned and no assignments to a notification team.

Local Administrators can:

- create Groups at Office level;
- enable their Office or Group assigned to their Office;
- disable their Office or Group assigned to their Office; and
- delete a Group assigned to their Office, provided that it has no users assigned and no assignments to a notification team.

Navigate to the 'Groups'-tab in the Access Management module, click the three dotted menu (point 1, Figure 38) and click 'Disable' (point 2, Figure 38).

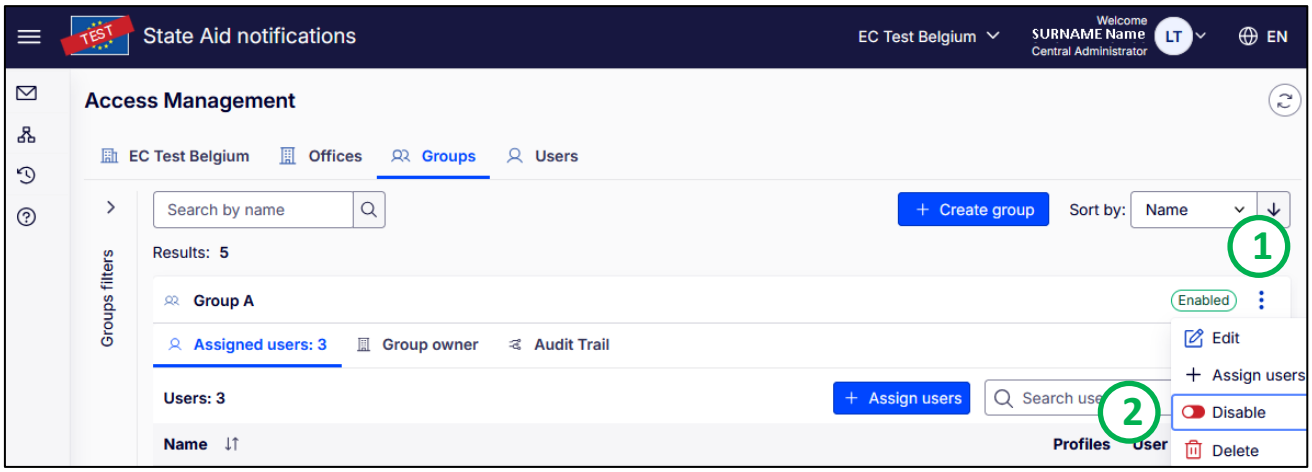


Figure 38: Disable a Group

The 'Disable group'-window opens. Provide the reason for disabling the Group and click the '**Yes**'-button to confirm (Figure 39).

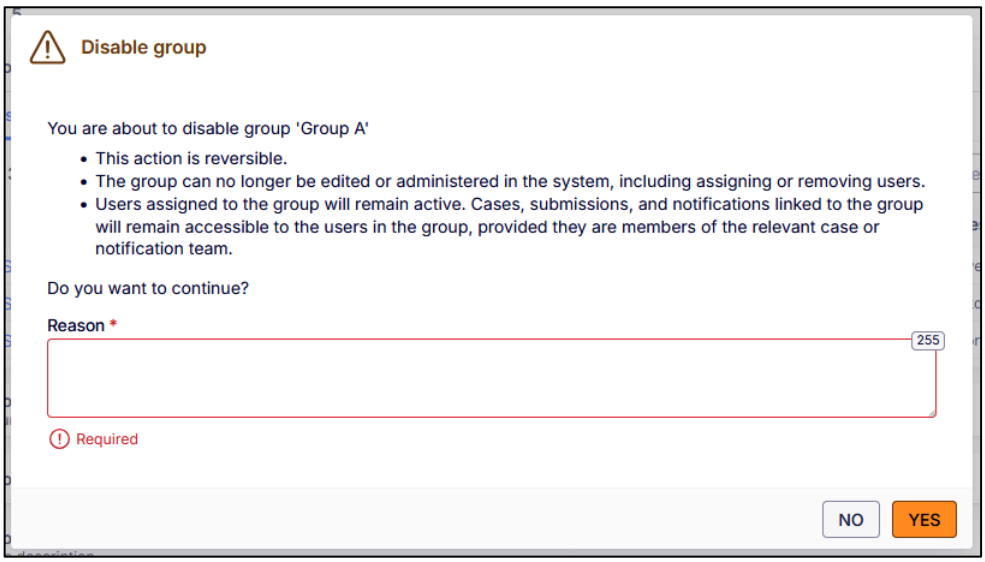


Figure 39: Disable a Group - Confirmation message

6.3.5.2. Enable a Group

When a Group is enabled, its information can be updated, users can be removed or assigned to it and the Group can be assigned to a Notification Team (Assign a Group of Users to a Notification Team).

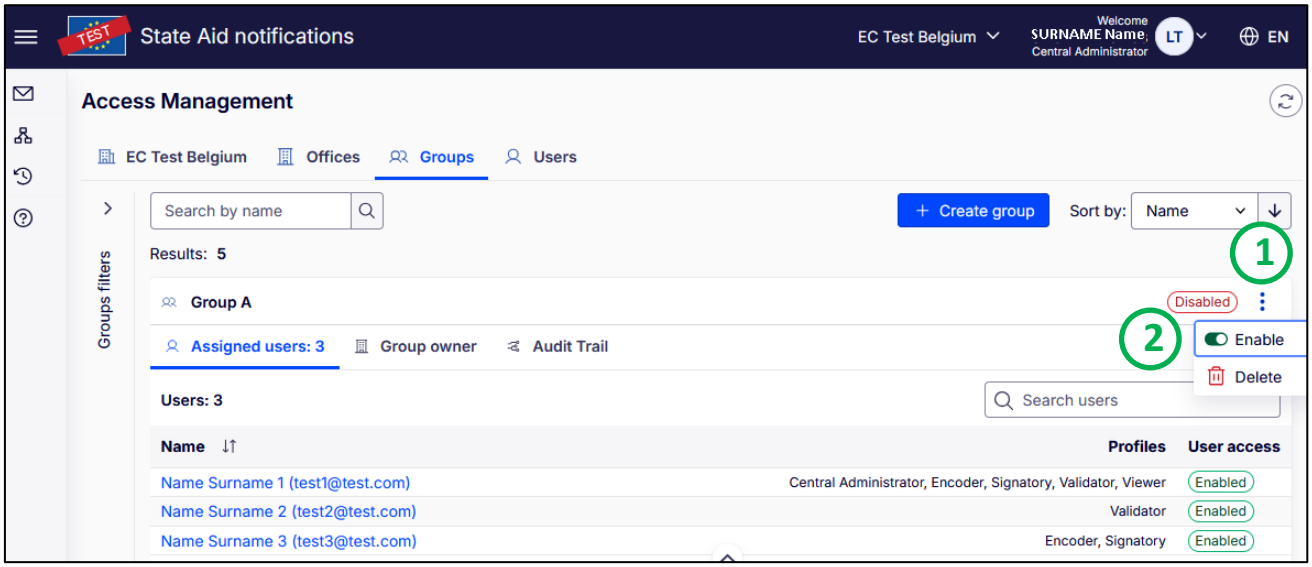


Figure 40: Enable a Group

Provide the reason for enabling the Group and click the 'Yes'-button to confirm (Figure 41).

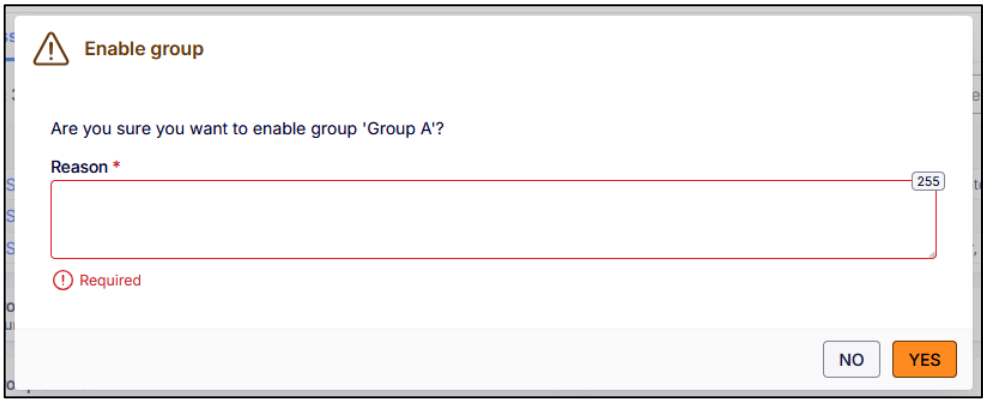


Figure 41: Enable a Group - Confirmation message

6.4. User management

Users are all individuals who need access to eNotifications, whether to manage other users, namely Central and Local Administrators or to create and manage notification forms. A user may have one or more profiles in eNotifications (see User profiles and permissions).

All user profiles including Central Administrators and Validators are created at Legal Entity level and can optionally be assigned to an Office and/or Group.

6.4.1. Create a user

If you are a Central Administrator or Local Administrator and wish to create a new user, click on the **'Users'** tab and (point 1, Figure 42) then on **'+ Create user'** (point 2, Figure 42).

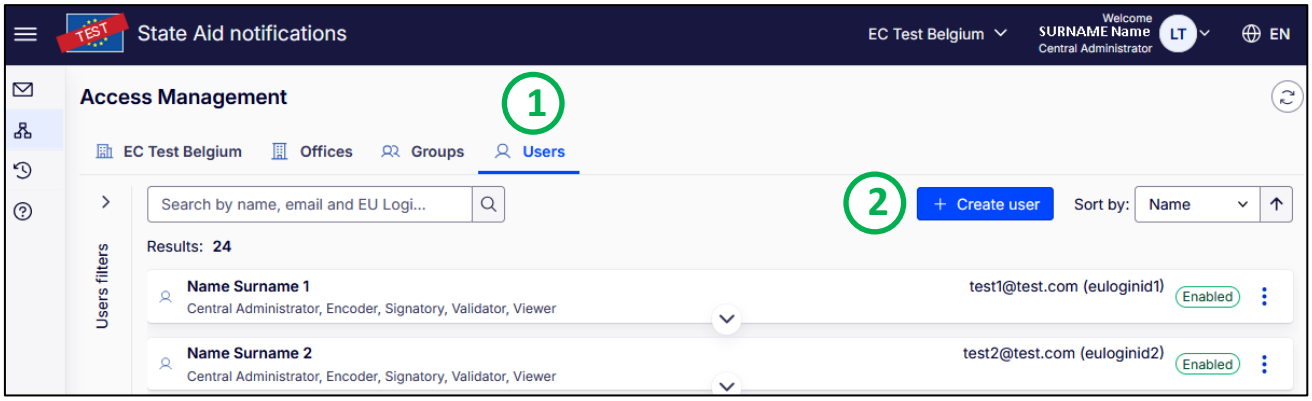


Figure 42: Create a user

The 'Search EU Login account'-window opens and allows you to search for an EU Login account using either an e-mail address or the EU Login username of the user to be created (Figure 43).

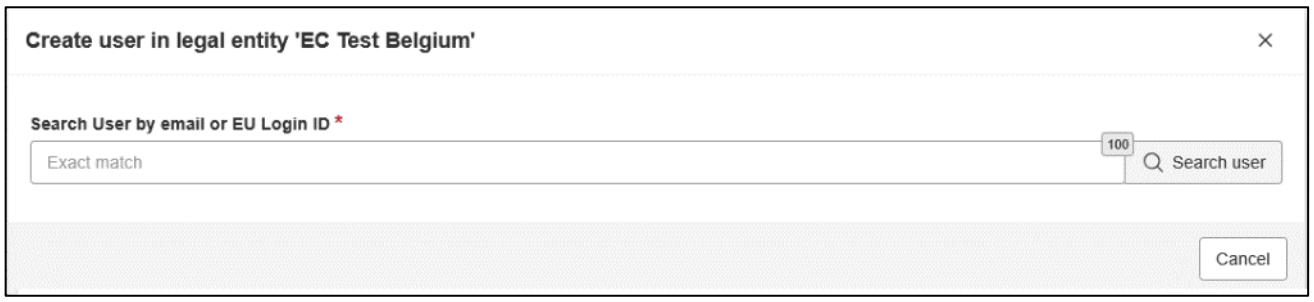


Figure 43: Create a user - Search EU Login account

Depending on the EU Login account search result, the Administrator will encounter of the below three scenarios.

6.4.1.1. Scenario 1: the new user has an EU Login account

If an EU Login account exists for the data provided, the account information will be retrieved as shown in Figure 44. At least one profiles must be assigned and, optionally, the user can be assigned to an Office. Click the **'Save'**-button to create the user in the system.

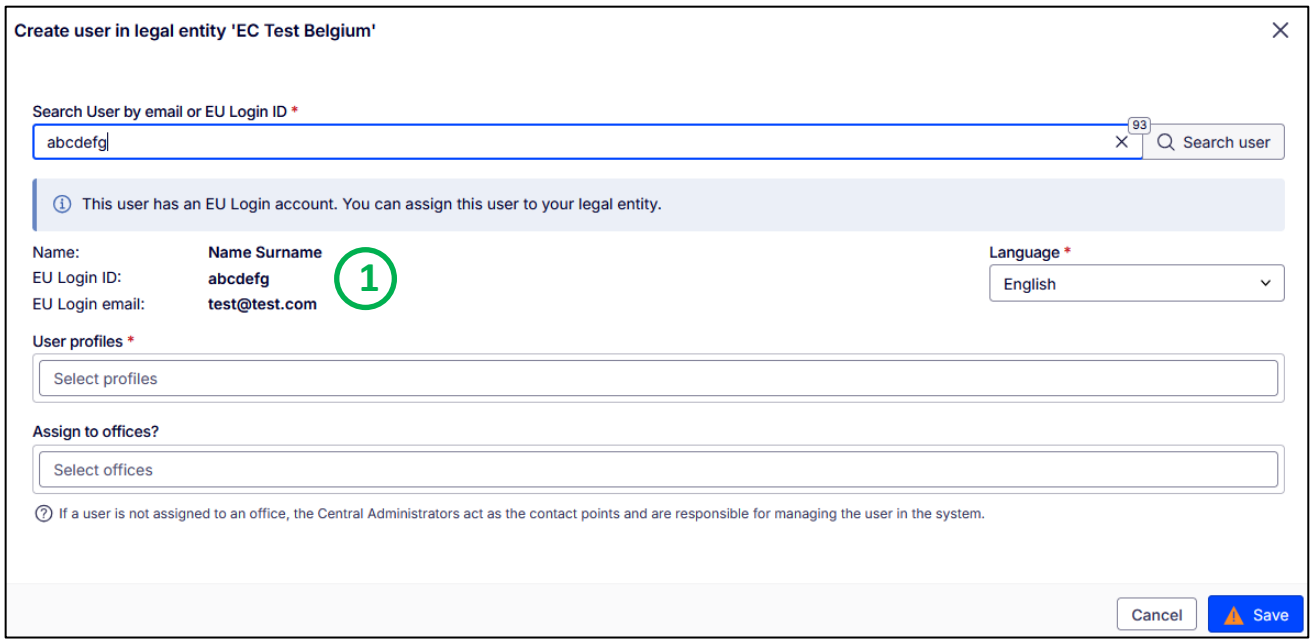


Figure 44: Create a new user - The new user has an EU Login account

As soon as access is granted, the user will be able to access the system according to the profile(s) granted to with no further action required. The user will also receive an informative e-mail (Figure 45) confirming that access has been granted. The contact information in the email is that of the user that created the new user.

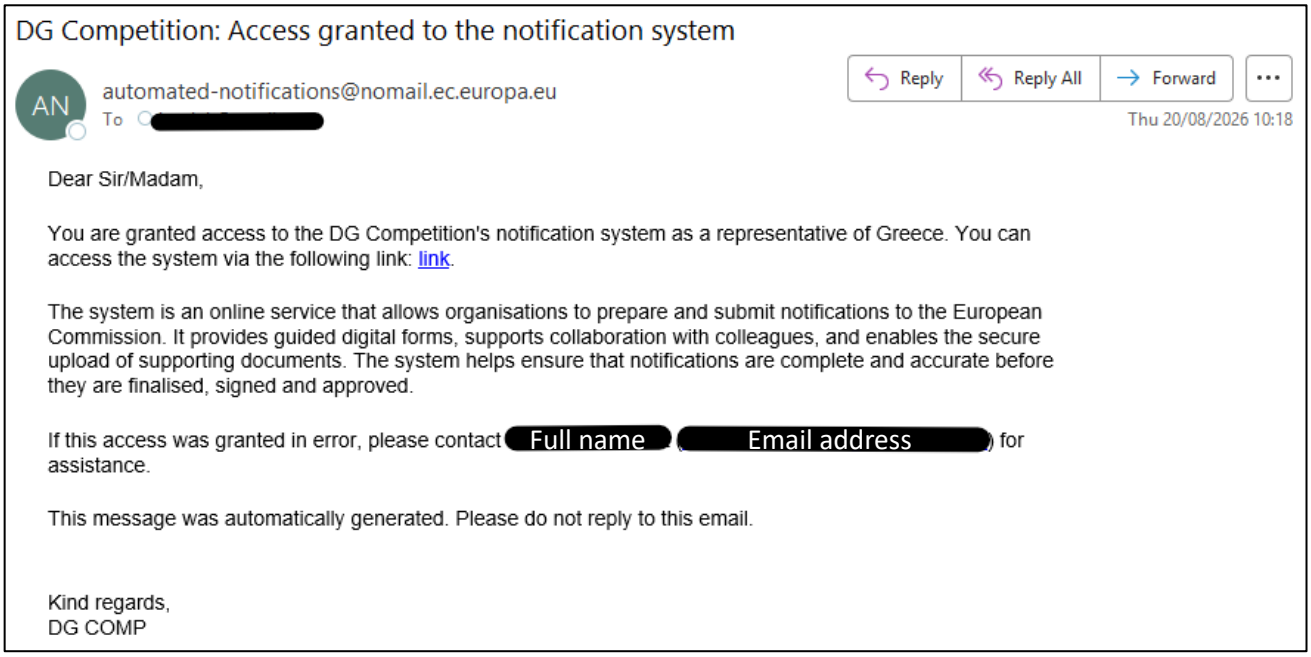


Figure 45: Email - A user with EU Login account is granted access to the system

6.4.1.2. Scenario 2: the new user does not have an EU Login account

Despite the new user not yet having an EU Login account, the Central Administrator or Local Administrator can still create the user, assign the necessary profiles (point 2, Figure 46), and assign the user to Office(s) and/or Group(s), where relevant. However, before the user can access eNotifications, they must create an EU Login account by using the email address provided here. The mandatory given and family name are used to address the new user in the registration email (Figure 47).

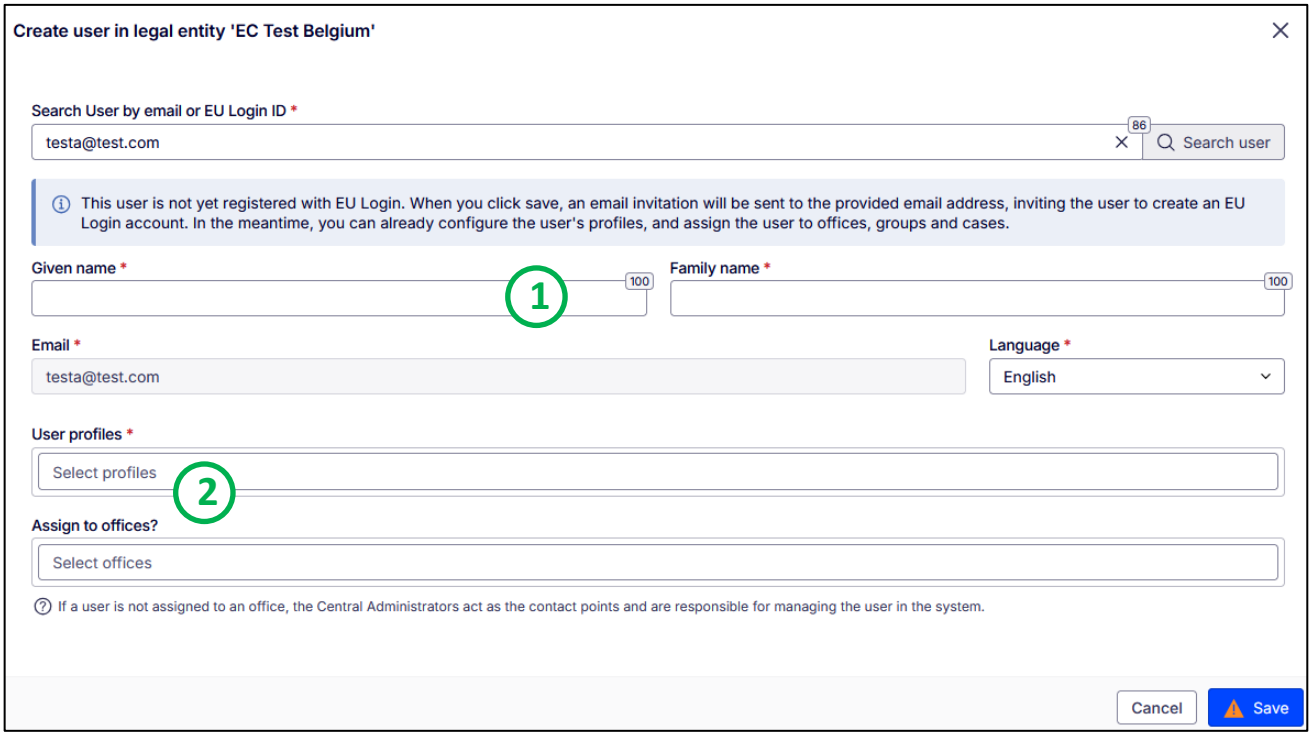


Figure 46: Create a user - The new user does not have an EU Login account

The user will receive an e-mail informing them that access has been granted and inviting them to create the EU Login account.

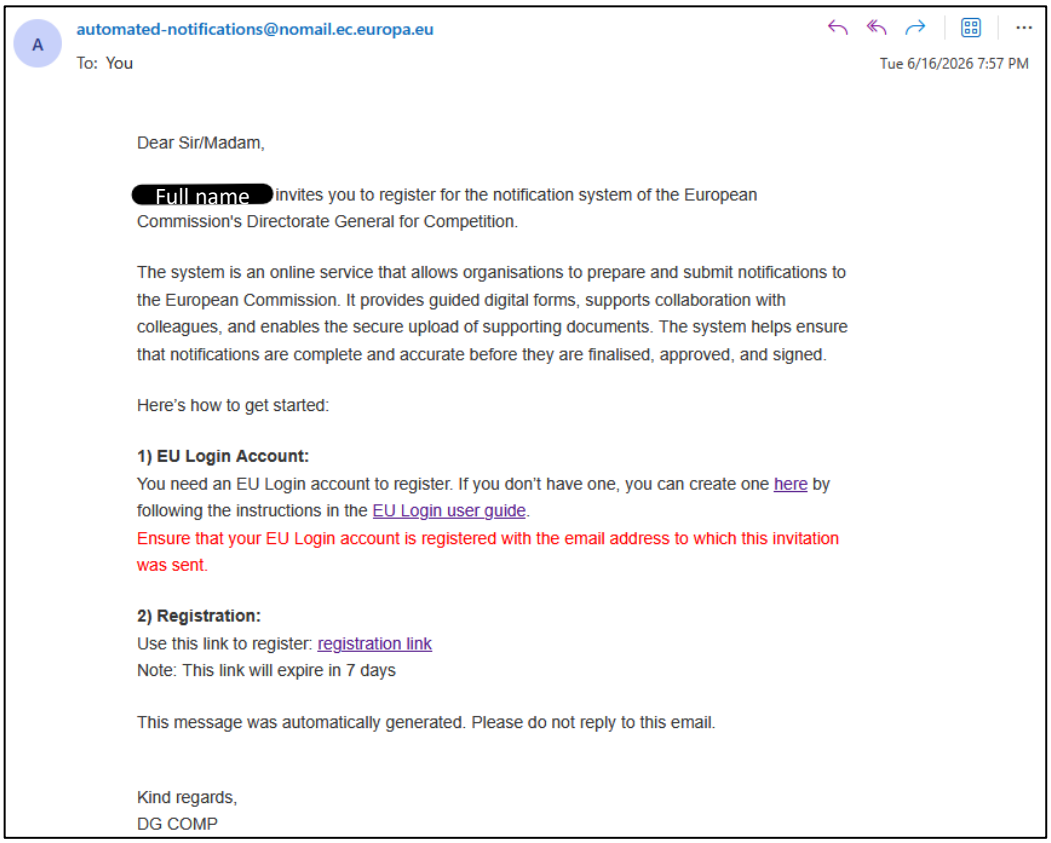


Figure 47: Email - User registration invitation

As long as the user has not created an EU Login account and confirmed their account in the system, they will appear as '**pending**' (point 1, Figure 48) in the users list. If the user does not complete the EU Login registration process within seven days the registration link expires. The administrator can resend the invitation by using the 'Resend registration invitation'-functionality available in the three-dotted (:) menu on the user (point 2, Figure 48).

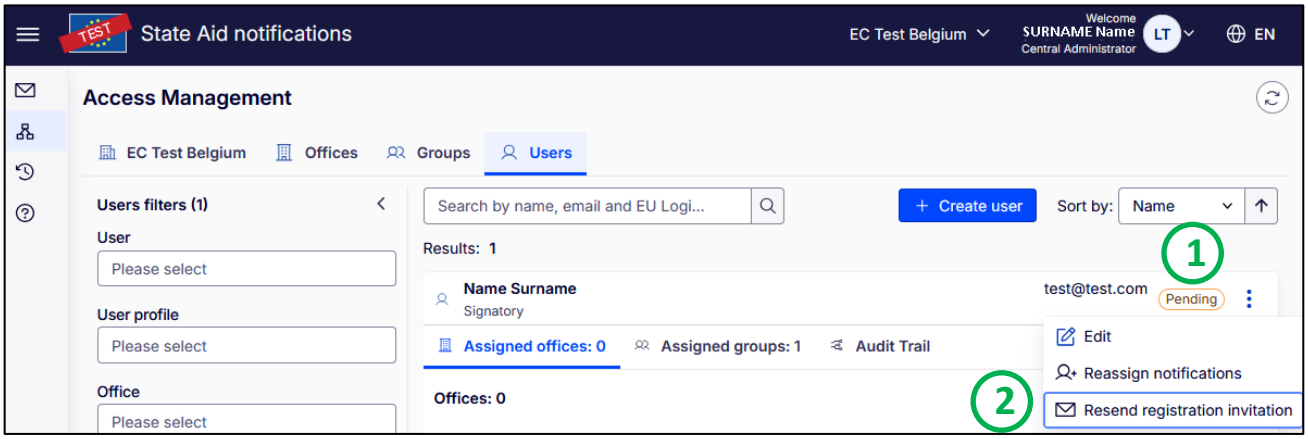


Figure 48: Resend registration invitation

6.4.1.3. Scenario 3: the user already has access to eNotifications

If the user to be created already exists in eNotifications, the Central or Local Administrator will be able to view, and if necessary, edit, that user's profiles and assignments by clicking the 'View user'-button (point 1, Figure 49).

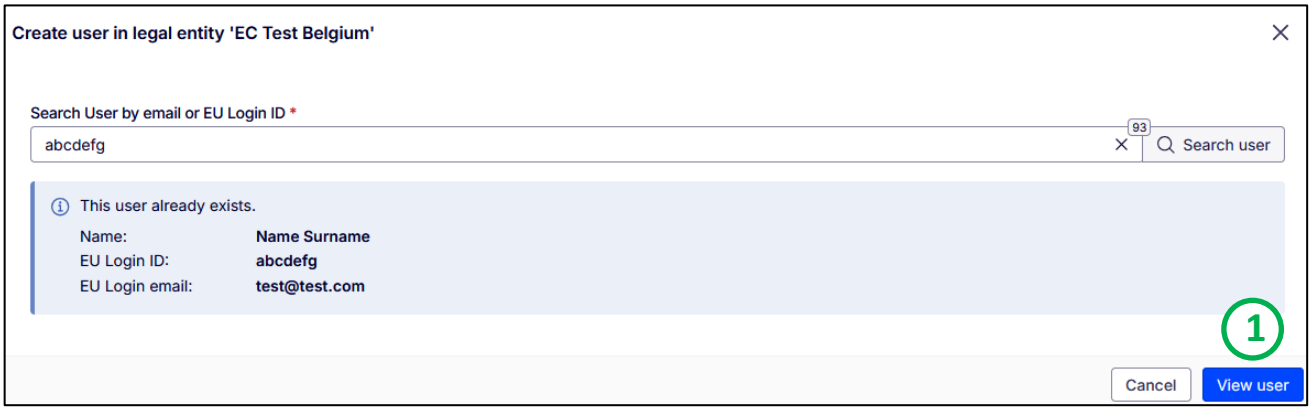


Figure 49: the new user is already registered in the system

6.4.1.4. Specifics when assigning the Validator profile to a user

In eNotifications, a user must be assigned to a notification team with one or more notification workflow profiles before they can access and contribute to a notification. The same applies to users who have been assigned the Validator profile (point 1, Figure 50). This differs from SANI2, where Validators did not need to be explicitly assigned to a notification team.

To reproduce the same behaviour as in SANI2 while complying with the new principles of eNotifications, it is possible to enable **the automatic assignment** of users with the Validator profile to notification teams. To do so, the Administrator must tick the checkbox labelled 'Automatically assign user to notification teams'. (point 2, Figure 50).

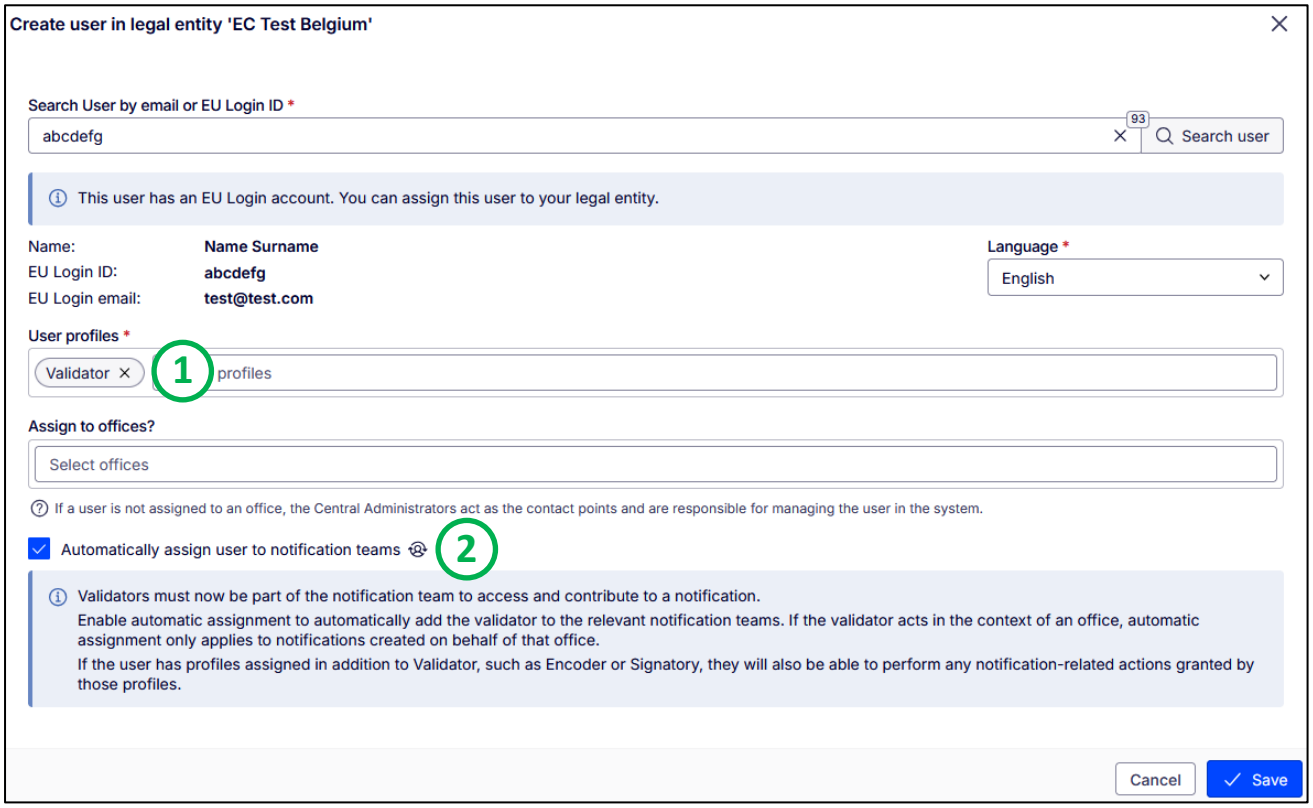


Figure 50: Automatically assign Validators to notification teams

Once this option is enabled, the Validator is added automatically to all relevant notification teams. If the Validator is assigned to a specific Office, the automatic assignment applies only to notifications created on behalf of that Office.

This can be useful, for instance, where a Member State or an Office operates with a single Validator. It is also useful where a given Validator needs to have access to all notifications from a Member State or an Office. In such cases, the Central Administrator or Local Administrator can choose to add this Validator to all notification teams by default. This means it is not necessary to add the Validator manually each time.

If the user also has other profiles, such as Encoder or Signatory, they also keep the notification-related permissions linked to those profiles.

6.4.2. Update user details

Central or Local Administrators can edit user details at any time by navigating to the user and click ‘Edit’ under the three dotted menu (point 1, Figure 51). This includes assigning or removing users to Offices (point 2, Figure 51) and Groups (point 3, Figure 51). However, EU Login-account related data, such as the e-mail address or name, can only be updated by users themselves in their EU Login account.

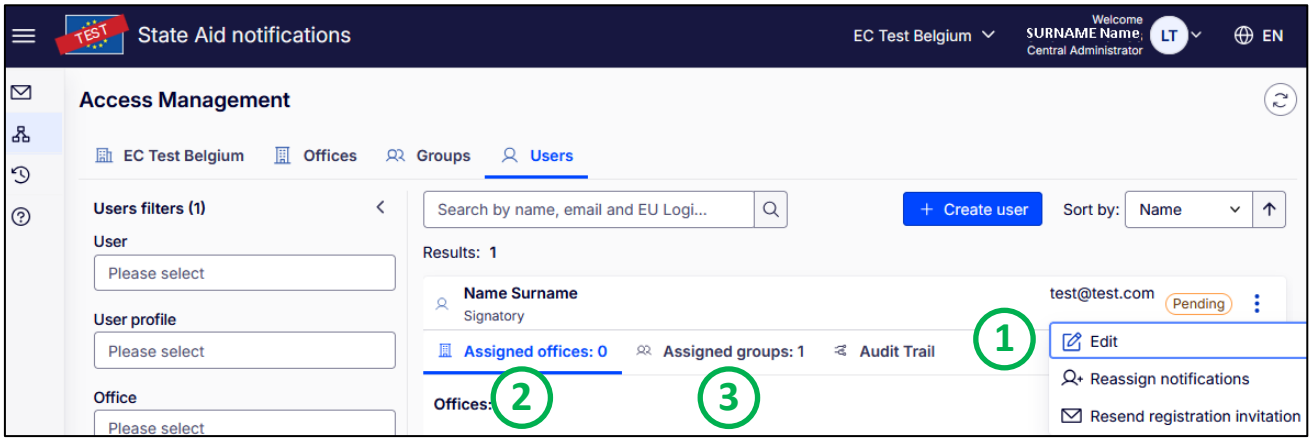


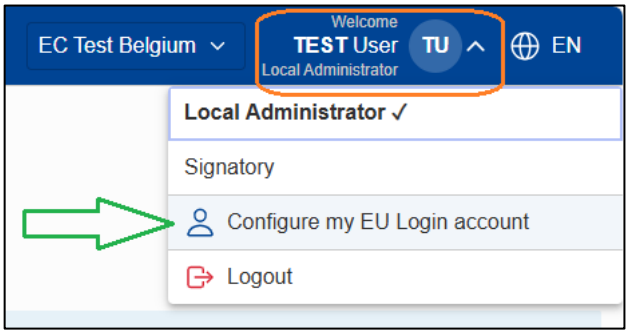
Figure 51: Updating user details

6.4.2.1. How to update a user's e-mail address or name

When necessary, for example, following a change to the e-mail domain or extension, users must update their own EU Login account details, such as their name or e-mail address, directly in their EU Login account. Therefore, if a user's e-mail address or name changes, the user should not be recreated in eNotifications, because the existing account remains valid once the EU Login details have been updated.

There are two available ways to update your EU Login account.

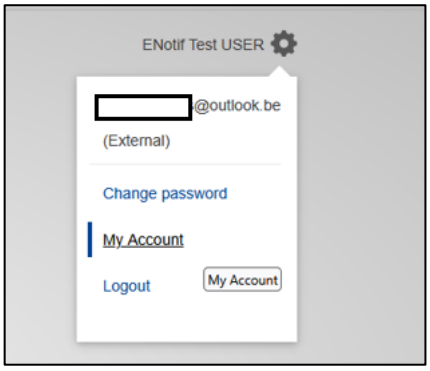
- quickly, directly from eNotifications, click on the drop-down arrow menu next to your name and select **'Configure my EU Login account'**:



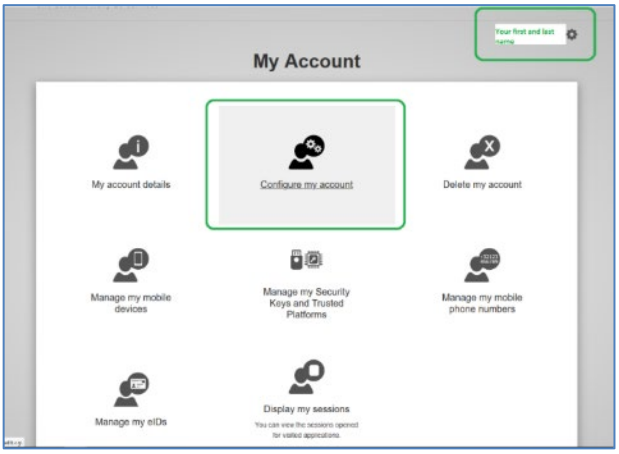
or

- sign in to your EU Login account using this link: https://webgate.ec.europa.eu/cas.

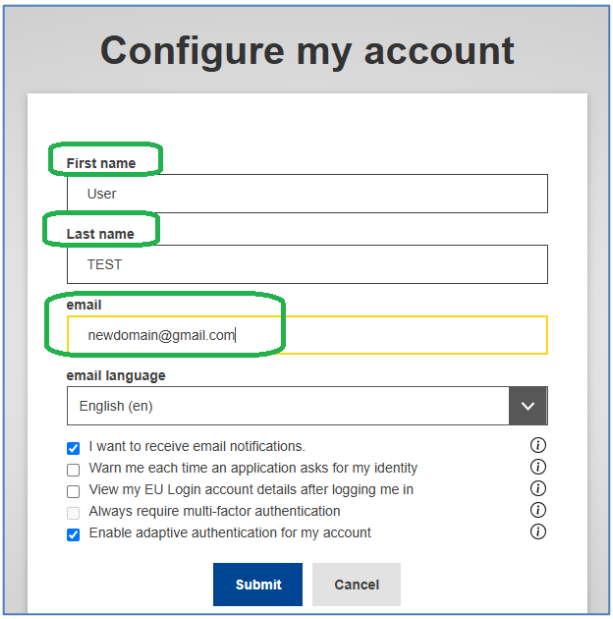
Once logged in to EU Login, click the settings wheel next to your name and click '**My Account**'



and then **'Configure my account'**



In the **'Configure my account'** window modify the relevant fields and click **'Submit'.**



Users' personal data is synchronised between EU Login and eNotifications. Therefore, all changes made in EU Login will be updated automatically in eNotifications.

6.4.3. Disable or enable a user

6.4.3.1. Disable a user

When a user is disabled, the user's access to the system is entirely revoked. Only the Central or Local Administrator can disable users. It is good practice to perform an annual user access review and to disable a user whenever his/her assignment changed to ensure that access is only maintained for authorised users.

Before confirming disabling the user, the administrator must provide a short justification. A disabled user can be re-enabled if necessary.

To disable a user, Central or Local Administrator access the user from the **'Users'** tab (point 1, Figure 52) and selects the option **'Disable'** (point 3, Figure 52) from the vertical three dotted (:) menu (point 2, Figure 52).

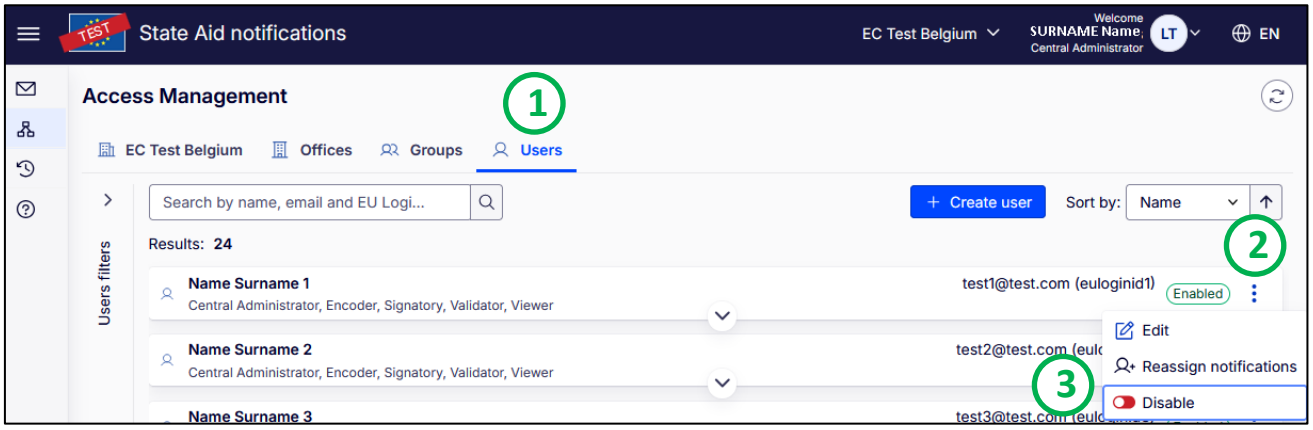


Figure 52: Disable a user

Before confirming the disabling action, Central or Local Administrators are required to provide a reason (Figure 53).

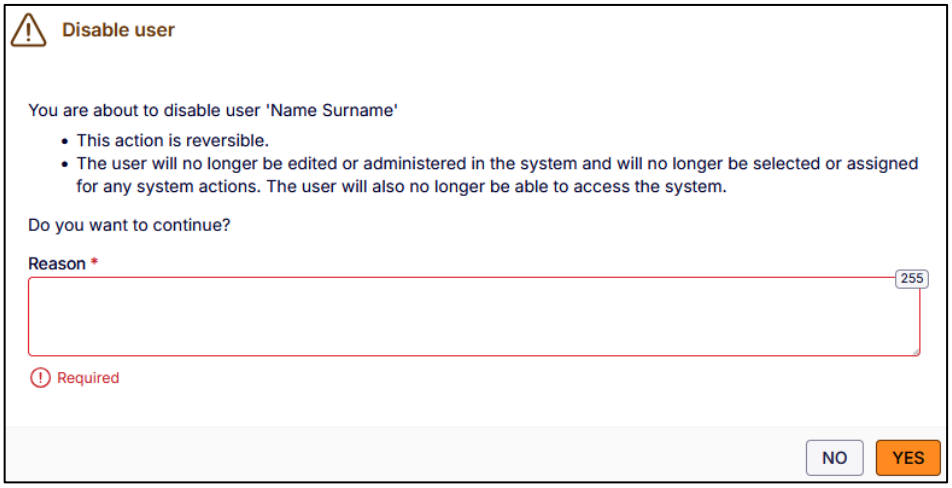


Figure 53: Disable a user - Confirmation message

6.4.3.2. Enable a user

When a user is enabled, the user's access to the system is entirely reinstated. This includes access to, for example, notifications to which the user was assigned to prior to being disabled. If that is undesirable, the user will need to be removed from the relevant notification team(s).

Only the Central or Local Administrator can enable users. To enable a user, access the user from the **'Users'** tab (point 1, Figure 54) and selects the option **'Disable'** (point 3, Figure 54) from the vertical three dotted (⋮) menu (point 2, Figure 54).

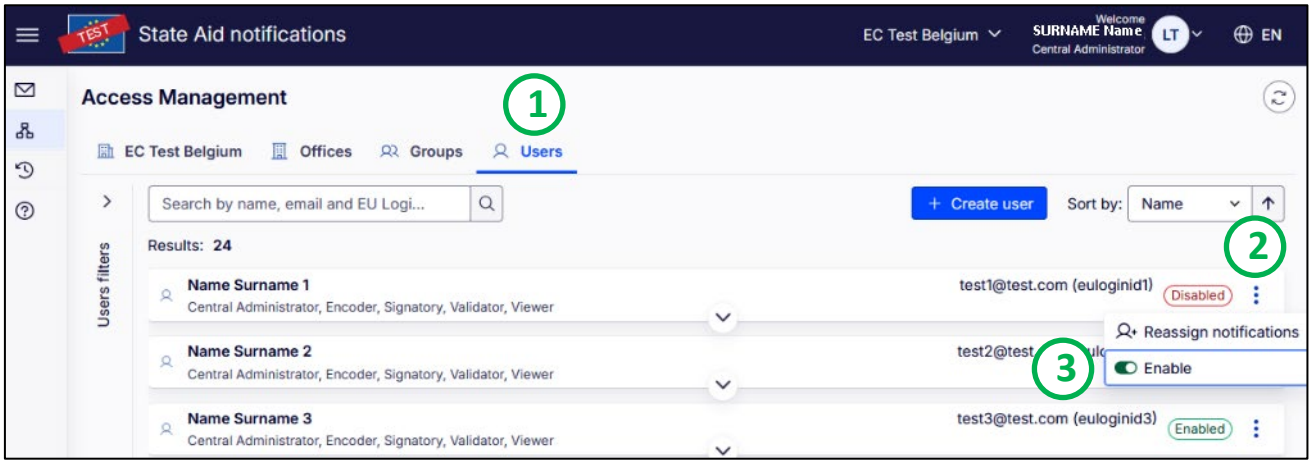


Figure 54: Enable a user

Before confirming enabling the user, the administrator must provide a reason ().

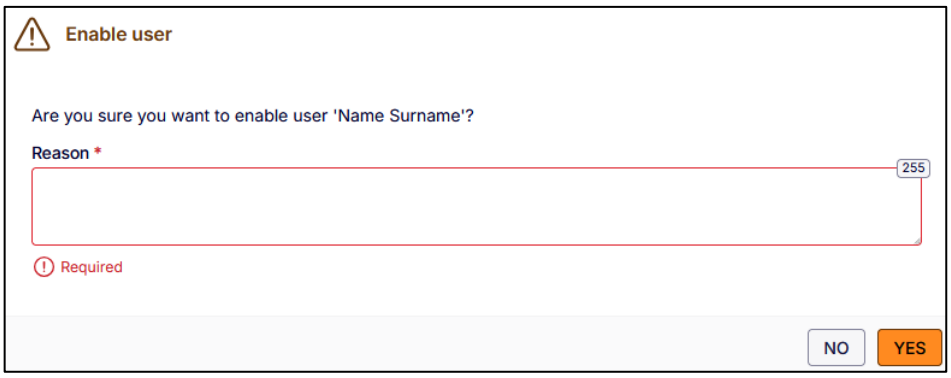
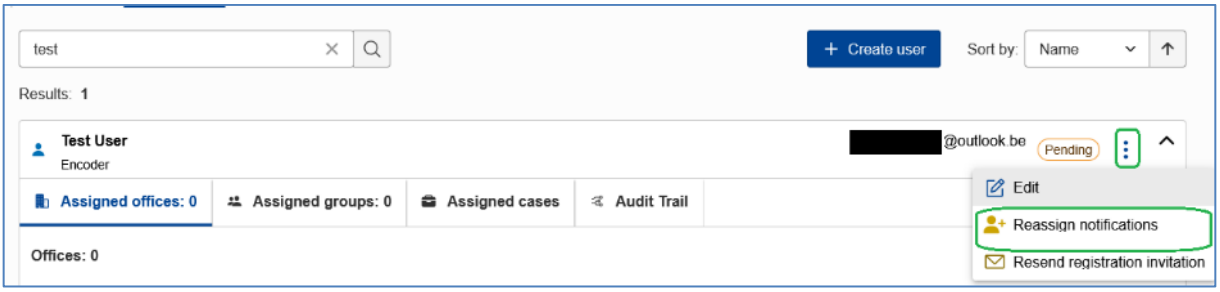


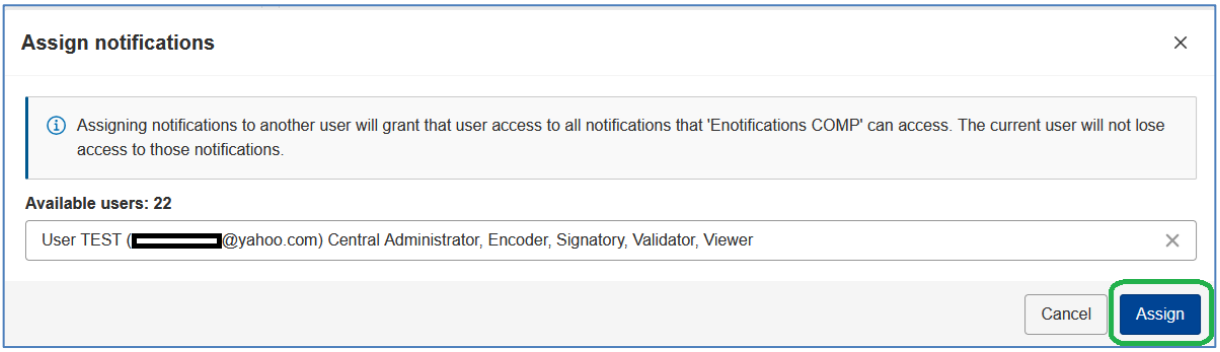
Figure 55: Enable a user - Confirmation message

6.5. Reassigning or sharing assignments between users

Central and/or Local Administrators can use the **'Reassign notifications'** function to give another user access to the notifications currently and/or previously accessible to a selected user. To do this, the Central or Local Administrator needs to navigate to the **'Users'** tab and click on the name of the user whose notification access is to be reassigned.



Select **'Reassign notifications'** and enter the credentials of the user who is to receive the same notification access or select that user from the list of **'Available users'**.



Important: this action copies-or shares the selected user's notification access with another user. It gives the recipient access to all notifications to which the original user has access. The original user keeps access to those notifications; access is not removed from that user. If the original user should no longer have access to eNotifications, that user must be disabled separately.

6.6. 'Audit trails' in the Access Management Module

The '**Audit Trails'** function allows Central Administrators or Local Administrators to consult a chronological record of actions carried out in eNotifications.

They are available to:

- Central Administrators, for the entire Legal Entity;
- Local Administrators, for the Offices to which they are assigned.

Its purpose is to provide transparency on who accessed or modified an item, and when the action took place. The Audit trails are intended to support:

- traceability of actions performed in the system;
- verification of access and assignment changes;
- monitoring of notification team management;
- administrative follow-up, where needed.

By consulting the audit trail events, users and administrators can better understand the history of a notification or of an access-management object and identify when specific actions took place.

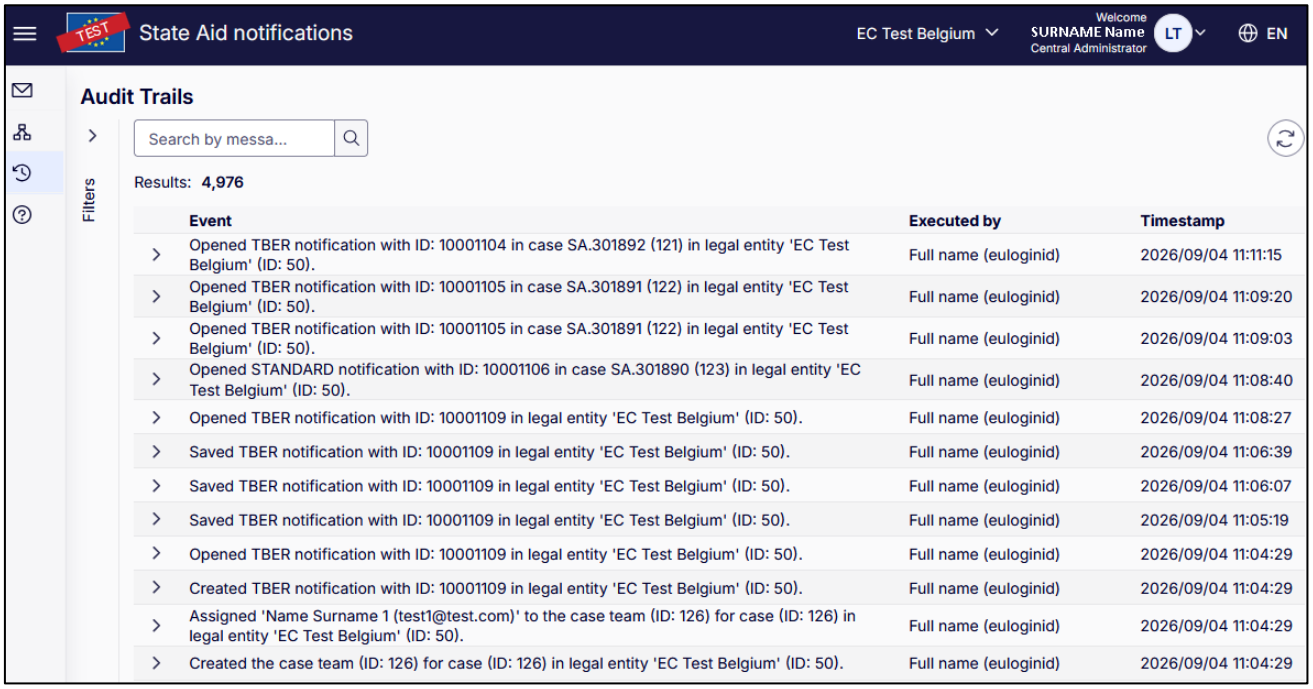


Figure 56: Audit Trail events in the Access Management module

Audit Trail events can be filtered based on the events that affected a selected Office, Group or User. It is also possible to filter by specific operations, within a selected timeframe, and to search for all events performed by a specific User. For the latter, the EU Login ID/username must be used, as the email address associated with an EU Login account can be updated and is therefore not unique.

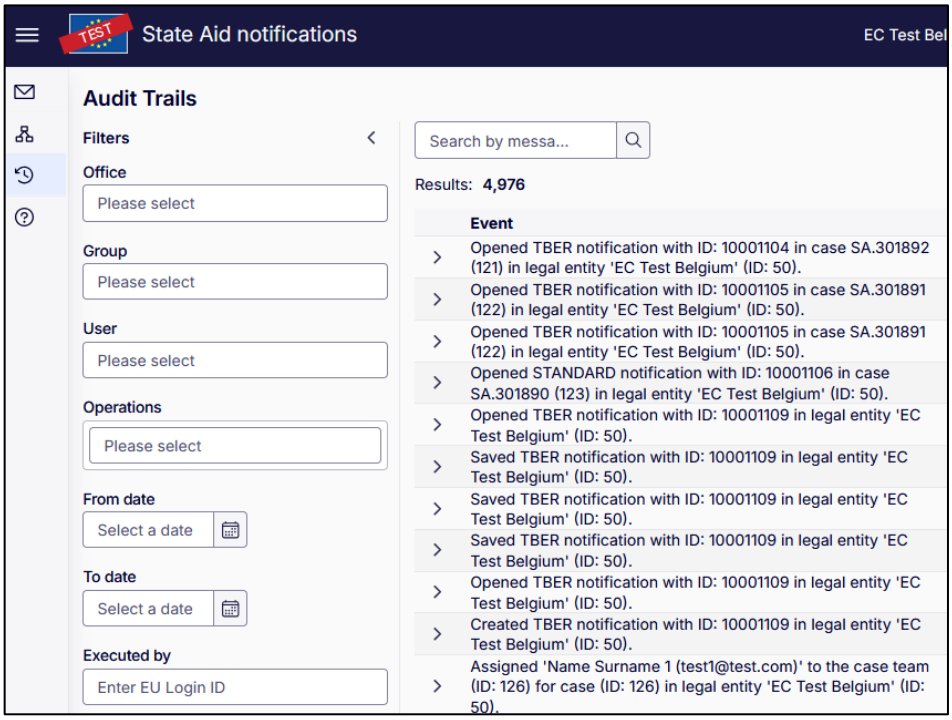


Figure 57: Audit Trail event filters in the Access Management module

7. THE NOTIFICATIONS MODULE

The Notifications Module is designed to allow Member States to submit new notifications to the Commission electronically as required by Regulation (EC) No 794/2004. All types of State aid related notification forms can be created and submitted via eNotifications. These electronic forms contain the information required in the forms that are annexed to relevant regulations.

This module is intended for users who participate in the notification workflow as detailed in section '8. Notification forms / information sheets - workflow'; Encoder, Signatory, Pre-validator, Validator and, where appropriate, Viewer.

The **'Notifications'** screen displays all the notifications, sorted by last modified date, that you have access to as a member of the notification team and based on the profile with which you are logged in (for details, see section '3.4. Login, user profiles and homepage'). To display the summary information of a notification, click the drop-down arrow icon on a notification.

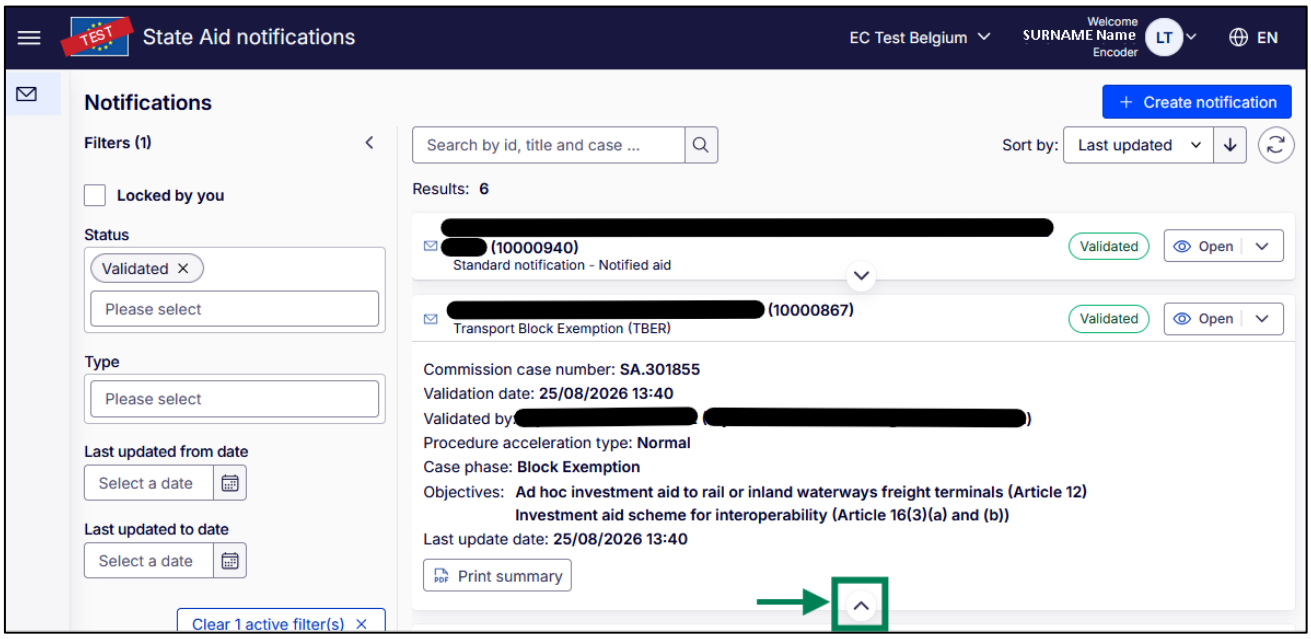


Figure 58: The 'Notifications list'-page with expanded summary information

7.1. Search function and filters available in the Notifications module

There are several ways to search for notifications.

As Encoder, Signatory, Pre-validator, Validator and Viewer, you can access only notifications if you are a member of the notification team. As Central Administrator or Local Administrator you can access all notifications for your Member State or Office. Do note that read-only access to the notification itself, depends on whether it is enabled for Central and Local Administrators, as explained in section '5.1.2. Setting for default read-only access for Central and Local Administrators'.

You can search on notification ID, title and case number simultaneously using the free text search field as shown in the screenshots below.

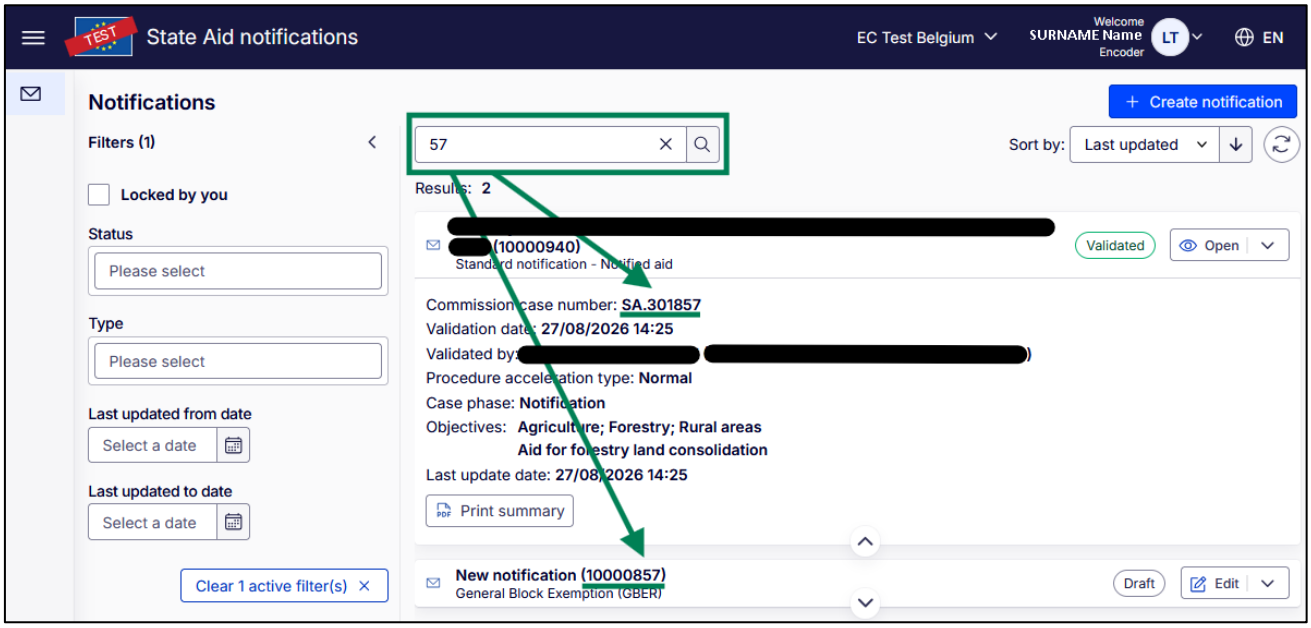


Figure 59: Search Notifications example

In addition to the search field, several types of filters are available in the Notifications Module. From the front page you can use the '**Sort by'** function to display results in a certain order. By default, the option is **'Last updated',** so the results always show the most recently modified notification first (point 1, Figure 60).

The **'Filters**' tab allows you to sort your notifications by:

- status of the notification form (the step the notification is currently) (point 2, Figure 60);
- type of form used for the notification (point 2, Figure 60);
- Filter on latest updated on date.

You can select multiple values from each filter and even combine different filters.

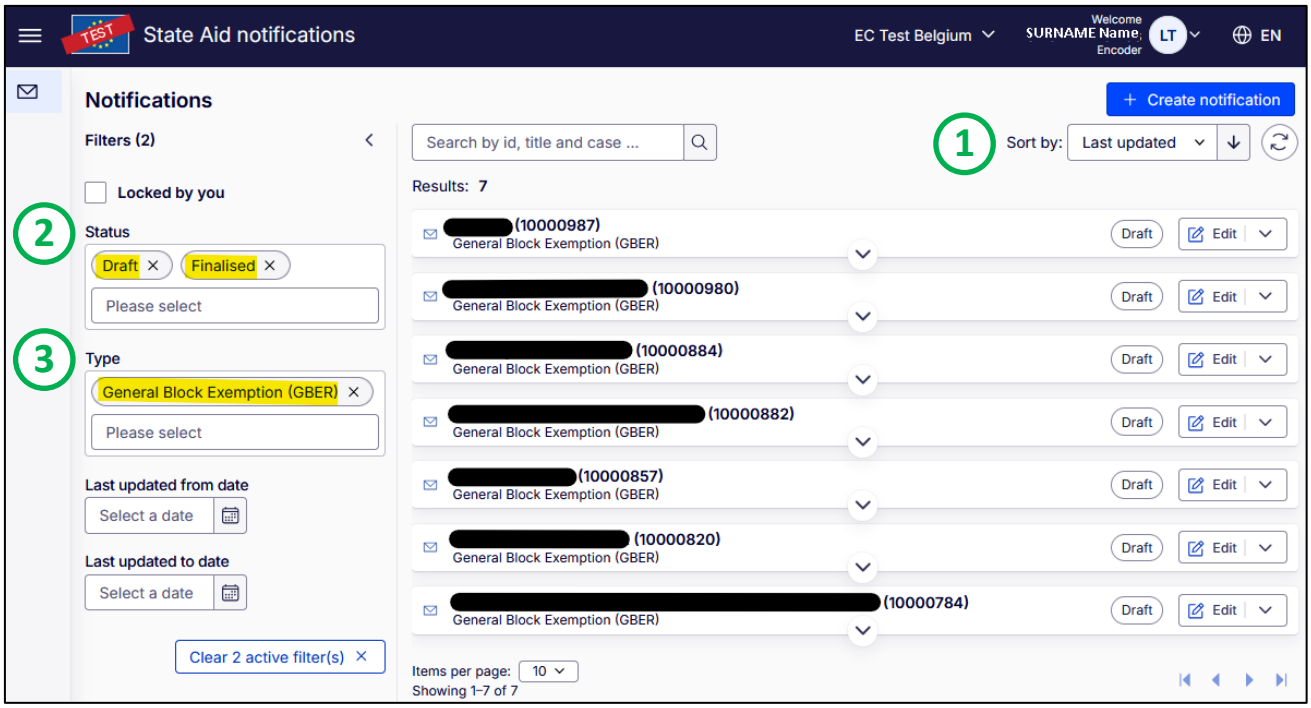


Figure 60: The 'Notification list'-page

7.2. Creating a notification

You can create new notifications only if you have an **'Encoder'** profile and are logged in with this specific profile. If you have several profiles, please switch to the Encoder profile, otherwise you will not be able to create a new notification.

To create a new notification, the Encoder clicks on **'+ Create notification'** button on the homepage.



Figure 61: Create a new Notification as Encoder

The 'Create notification'-window opens from which Encoders select the appropriate form to use for a given notification.

7.2.1. Creating a block exempted notification (GBER, ABER, FBER, TBER)

If a **block-exempted** form is selected, Encoders confirm the creation by pressing the **'Create notification'** button.



Figure 62: The 'Create Notification'-window

7.2.2. Creating a simplified notification

For the Simplified procedure Notification form, the Encoder is required to indicate the SA number allocated to the measure that is subject only to amendments allowed under Article 4 of Regulation (EC) No 794/2004.

An Encoder may create a simplified notification only if they are assigned to the Notification Team responsible for the standard notification linked to the prior approved aid number. If the Encoder is not a member of that original Notification Team, they will not be able to create a simplified notification for the prior aid number.



7.2.3. Creating a standard notification

7.2.3.1. Providing a SA reference / Case number

For the **Standard notification** form, before the Encoder can select the relevant variant of the standard form (notification, pre-notification, or notification for legal certainty), they are required to indicate if the State aid reference (**Commission SA number**) already exists.

Indeed, in the case of preliminary or pre-notification contacts with the Commission, such number will already be allocated to the measure. By indicating it in this field Encoders will ensure that the notification form is automatically linked to the initial case and is therefore registered by the Commission under the same SA reference. Please enter the correct SA reference in this field. If there were no preliminary discussions with the Commission about the measure at stake, please select **'No'**.

Providing the SA reference is particularly important, as it ensures that related information is registered in the correct case and allows the notification to be processed correctly and efficiently.

If a notification is created following the submission of a pre-notification, it can only be created when all of the following conditions are met:

- the pre-notification has reached "Validated" status;
- no other notification exists for that pre-notification;
- the encoder is a member of the Notification Team for that pre-notification.

If the pre-notification was **submitted through the system**, the system will automatically load the relevant data to facilitate drafting and submission the notification. If the pre-notification was submitted to the Commission

outside the system (for example, by email), the data cannot be loaded automatically and must be entered manually.

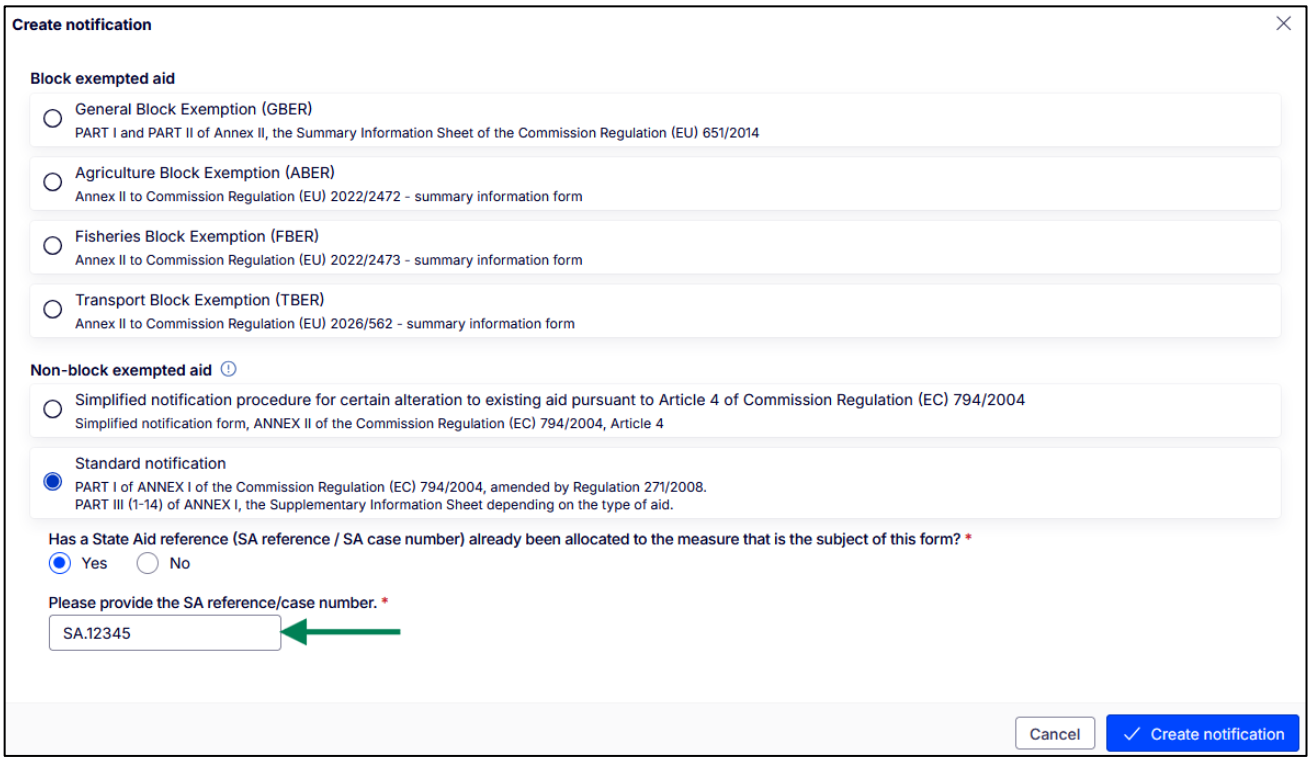


Figure 63: Create notification - Standard notification: provide SA reference

Please note that for notifications or pre-notifications concerning amendments to existing measures that exceed the conditions for the simplified notification procedure under Article 4(2) of Regulation (EC) No 794/2004 you should also select 'No', as the Commission will allocate a new case number.

7.2.3.2. Selecting the standard notification 'variant' (pre-notification, notification, legal certainty)

Please note that, in line with Annex I of the Regulation (EC) No 794/2004, for 'Standard Notification' you will be able to select the appropriate notification variant (**notification, pre-notification** or **notification for legal certainty**) under the first section of the **'Standard notification'** form.

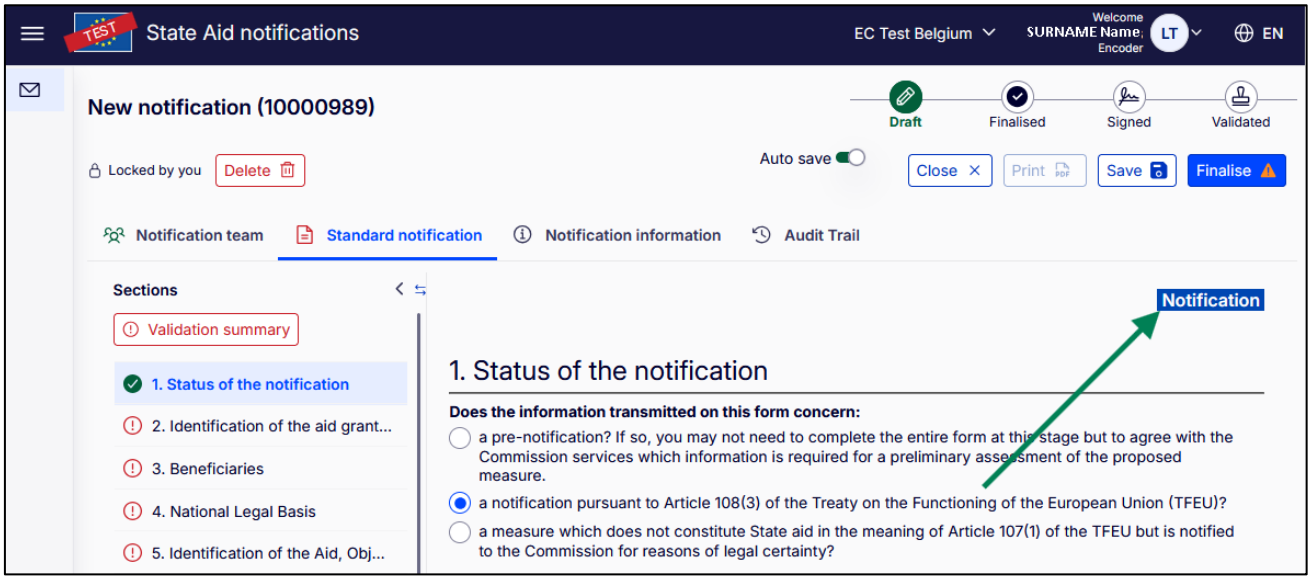


Figure 64: The standard notification - Select the notification variant

7.3. Setting up a Notification Team

Any notification or summary information sheet submitted to the Commission consists of four steps, or five, in countries that include the pre-validation step for the Standard Notification Form: **Draft, Finalised, Signed** and **Validated**. These steps are described in detail in section '8. Notification forms / information sheets - workflow'. To process a notification successfully through these steps, several actors with appropriate access rights are required. It is therefore necessary to set up the notification team properly before it can be 'Finalised'. When a new notification is created, the system checks whether the necessary profiles, notably Signatory and Validator, are present in the notification team.

The 'Notification team' can be modified by any member of that notification team throughout the workflow. The Central Administrator, or where applicable the Local Administrator, may also use the function described in section '5.5. Reassigning or sharing assignments between users' where broader access to notifications needs to be shared with another user.

Please note that, to be assigned to a Notification Team, a user must have at least one notification workflow profile assigned, i.e.: Viewer, Encoder, Signatory, Pre-validator, or Validator (see Section 4.2.). Users who only have the Central Administrator or Local Administrator profile cannot be assigned to a Notification Team.

7.3.1. The notification team overview

The screenshot below shows the "Notification team overview" in the **'Notification team'** tab. It gives a clear overview of which users are assigned to the notification team but also which role and permissions they have for the notification. It also shows whether users are assigned to the notification team automatically, as individual users or as member of a group.

- indicates users who have been **automatically assigned** to the notification team in accordance with their user settings. Only users with at least the **'Validator'** profile can be configured for automatic assignment to the notification team (see section '5.4.1.4. Specifics when assigning the Validator profile to a user').

- indicates users who have been manually added to the notification team as **individuals**.

indicates users who have been manually added to the notification team as members of a **group**.

If a user has multiple profiles assigned, that user will be displayed under each relevant profile.

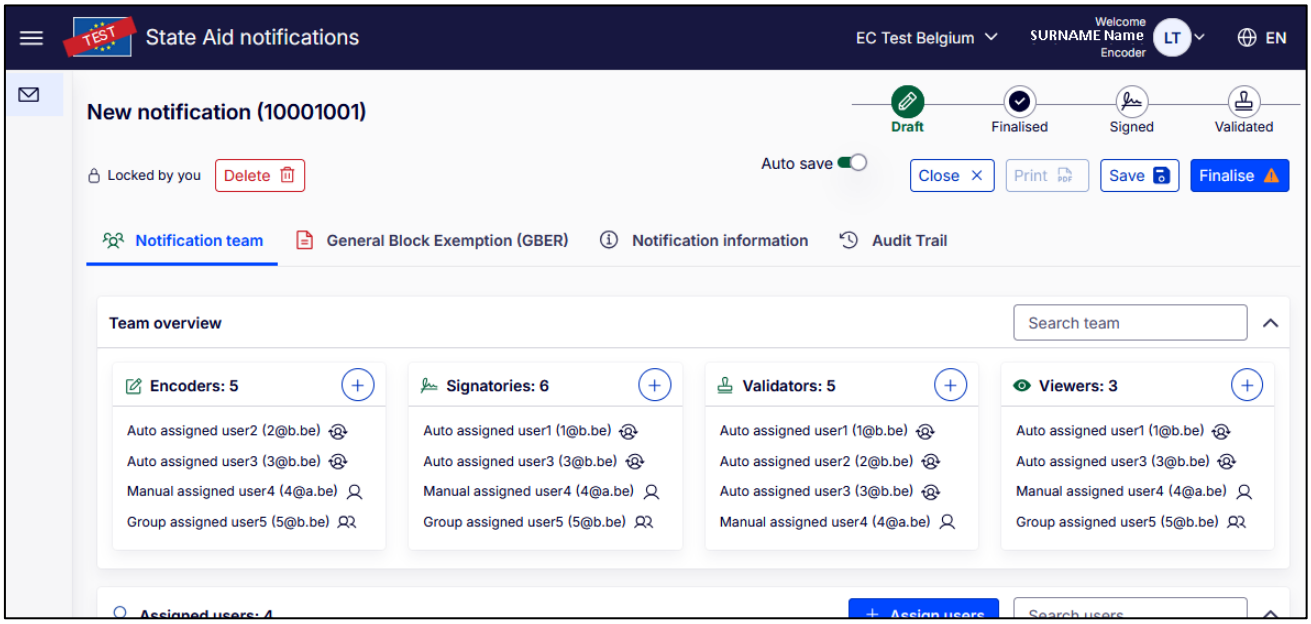


Figure 65: Notification Team overview

The overview also provides information on the completeness of the notification team. This is necessary to make sure that there is at least one user that has the permission to proceed with the next step in the notification workflow.

- Green coloured profiles indicate that one or more valid users have been assigned.
- Red coloured profiles indicate that no users have been assigned. A user assignment is mandatory before the notification can move to the next step.
- Orange coloured profiles indicate that no users have been assigned. This does not prevent the notification from moving to the next step, because that profile is not required to act at that stage. However, assigning a user will become mandatory later in the process.

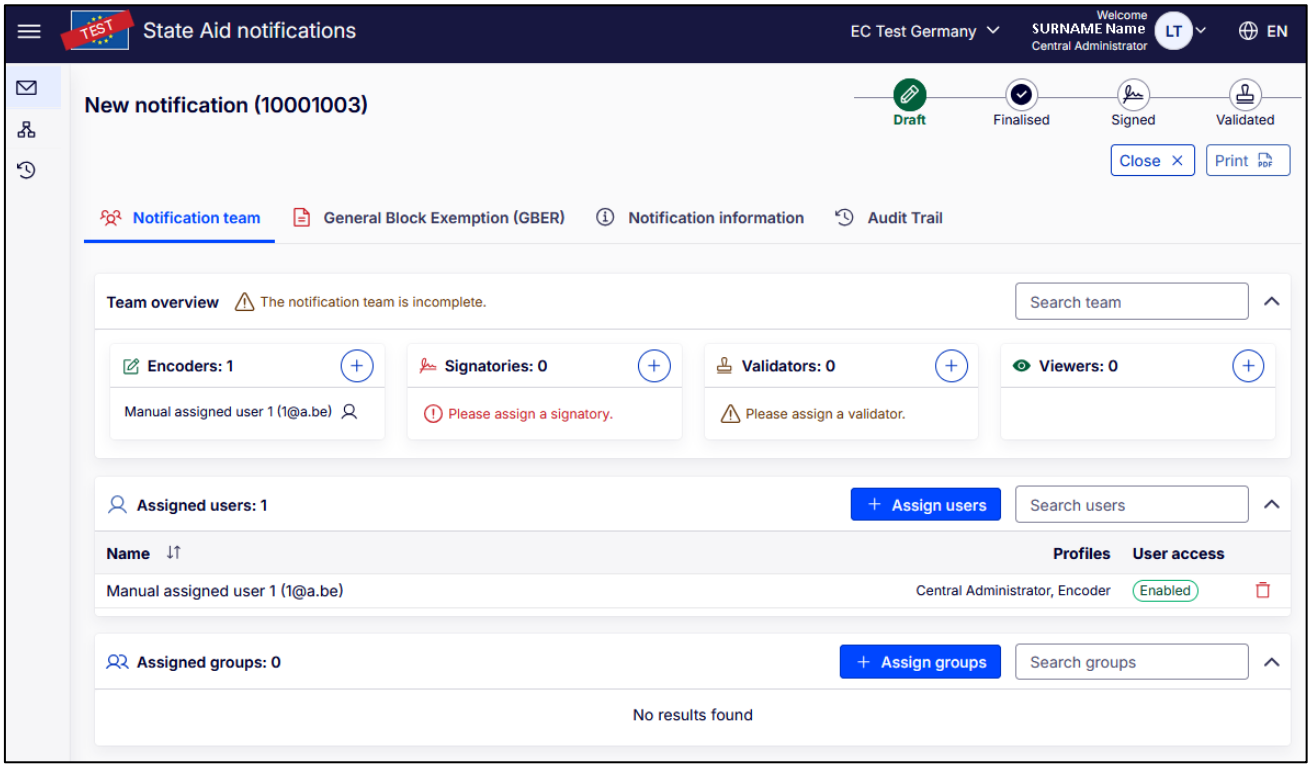


Figure 66: Notification Team overview - Team completeness

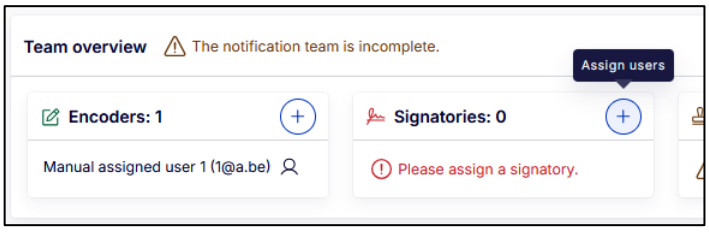
In the example shown in Figure 66, assigning at least one user with the Signatory profile to the Notification Team is mandatory (indicated by the red colour and messages). Since the notification is in 'Draft' status, a Signatory is required once the notification is finalised by the Encoder. The Validator profile remains optional at this point but will be mandatory when the notification needs to be signed and thereby handed over to the Validator.

Below the notification team overview, there are the functionalities that enable you to fully manage the assigned users and groups (Figure 66).

7.3.2. Assigning users to a notification team

7.3.2.1. Assign individual users to a Notification Team

eNotifications also allows individual users to be added to the team for any notification. This can be done directly via the 'Notification team'-tab by clicking the **'+'** icon next to the profile for which a user is to be added.



When using this option, the system **automatically filters** the **users** that have at least the **selected profile** (point 1, Figure 67). To search for a user, place the cursor in the 'Search…' field (point 2, Figure 67). You can search and add as many users as needed before clicking the "Assign"-button to confirm (point 3, Figure 67).

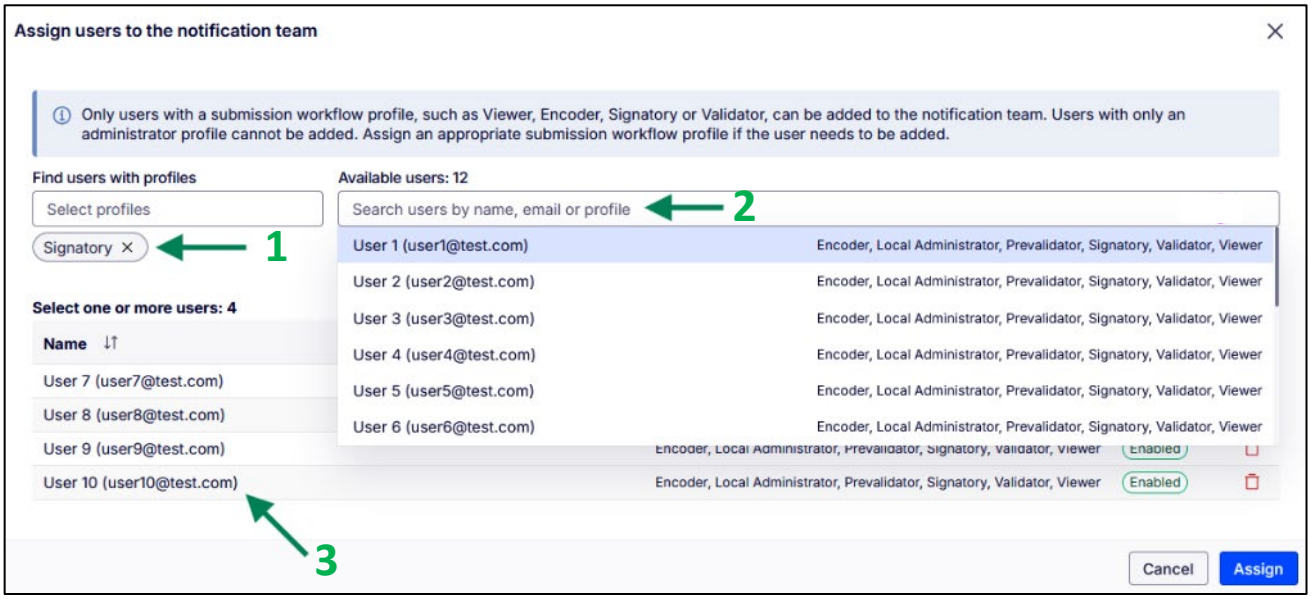


Figure 67: Assign user(s) to the Notification Team

Note that if a user is disabled, that user will not be able to access the system and therefore notification. Disabling a user does not automatically remove that user from the notification team (Disable a user). Whether a user is enabled or disabled is reflected in the 'User access' column.

Users can also be added through the **'+ Assign user'** function, which allows searches by profile, name, or e-mail address. The exact same window opens as the one depicted in Figure 67. The only difference is that no profile will be preselected (point 1, Figure 67).

7.3.2.2. Assign a Group of Users to a Notification Team

In addition, several users can be added at once through the **'+ Assign groups'** function. See also section 'Group management' for an explanation of the purpose and management of Groups.

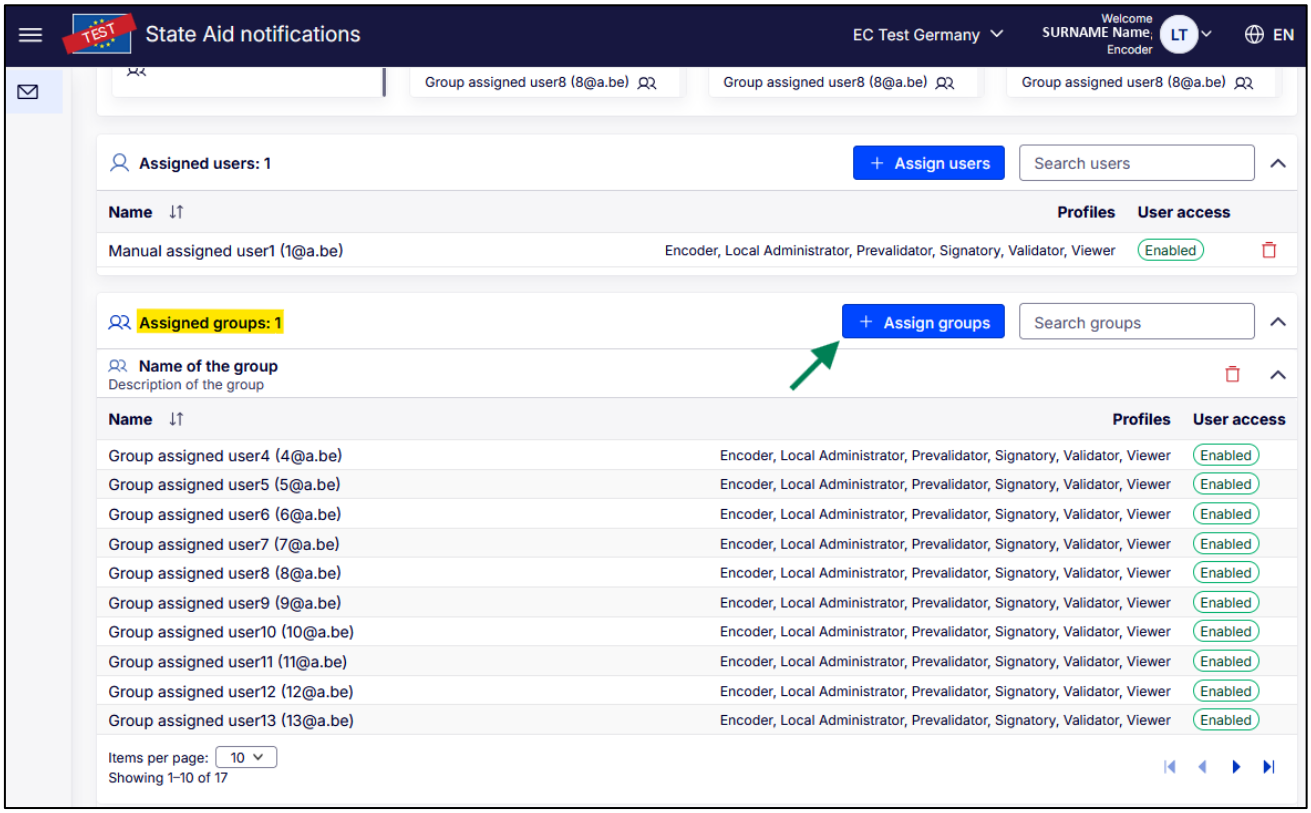


Figure 68: Assign (a) Group(s) to the Notification Team

Search for the Group(s) you want to assign and click 'Assign' to confirm (Figure 69).



Figure 69: Assign (a) Group(s) to the Notification Team - Search and select Groups

7.3.3. Removing users or groups from a notification team

Whenever necessary a user or a Group of users can be removed from the notification team. The user removed will be notified that their access has been revoked. Similarly, a group can be removed from the notification team. By removing a Group, the access to the notification is revoked for all users of that Group.

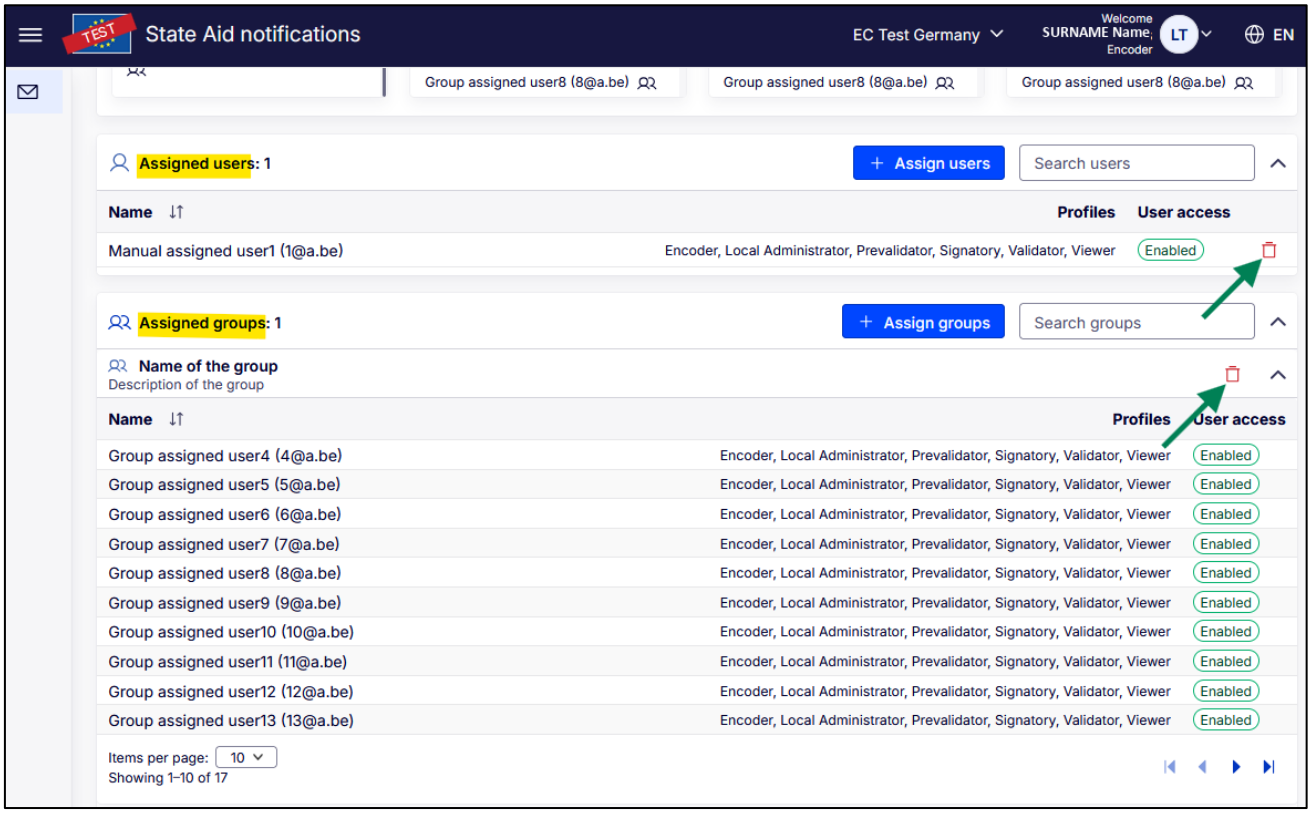


Figure 70: Removing users and Groups from a Notification Team

7.4. Drafting a notification form – 'Notification form page'

The instructions below explain how users should complete a notification form, from entering information in each section to checking that all required information is provided correctly before submission. They guide users through the practical rules for filling in the form, including how mandatory questions and fields are identified, how additional fields may appear depending on the selected answers, and how validation messages help users detect and correct missing or incorrect information.

When you open a notification, the left panel (point 1, Figure 71) lists the different sections of the form. The right side (point 2, Figure 71) shows the form of the selected section. The left panel can be collapsed by clicking the **<** icon or the width can be adjusted by clicking the vertical separator and dragging it to the desirable width (point 3, Figure 71 and point 1, Figure 72).

Some questions or fields are mandatory. Sections containing such mandatory elements are displayed with a red warning icon (point 1 in Figure 71) until all mandatory questions have been answered.

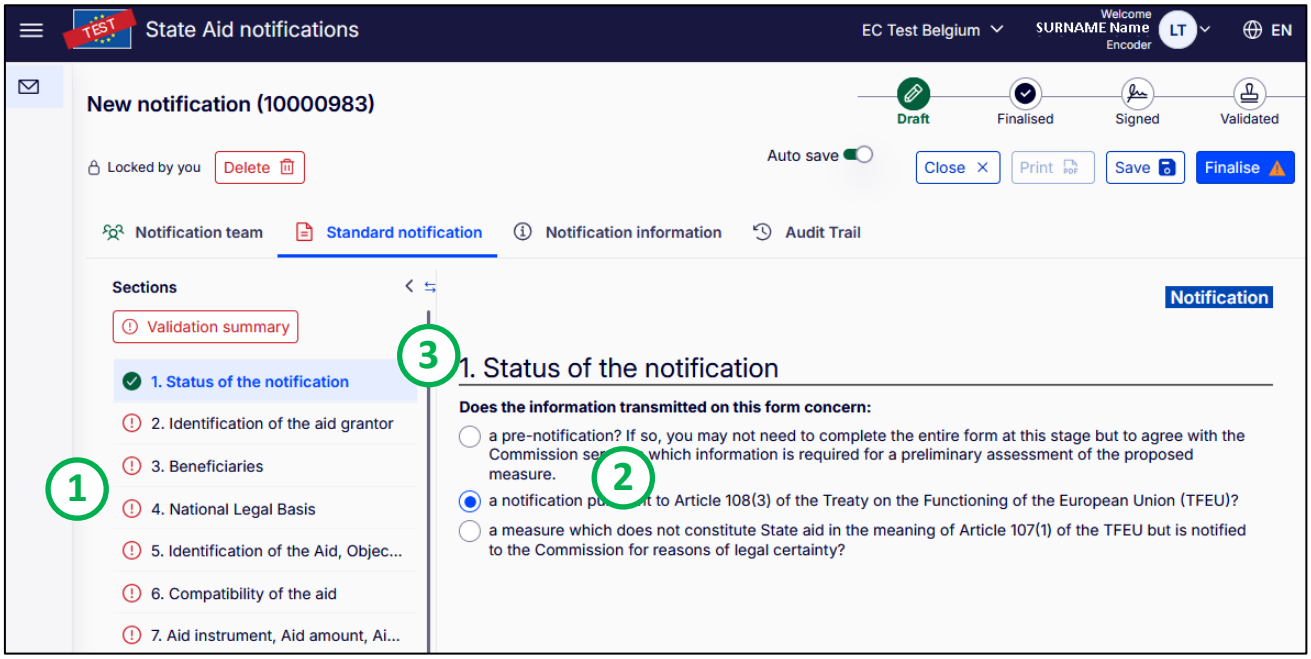


Figure 71: notification form layout

Please note that, for the standard notification, it is possible to change the variant (i.e. pre-notification, notification or notification for reasons of legal certainty) of the notification until it has been 'Finalised' by selecting another option from the list in Section 1 (point 2, Figure 71)). Changing the variant of the notification will add or remove certain questions and mark or unmark some fields as mandatory. An example of mandatory fields is displayed in point 2, Figure 72.

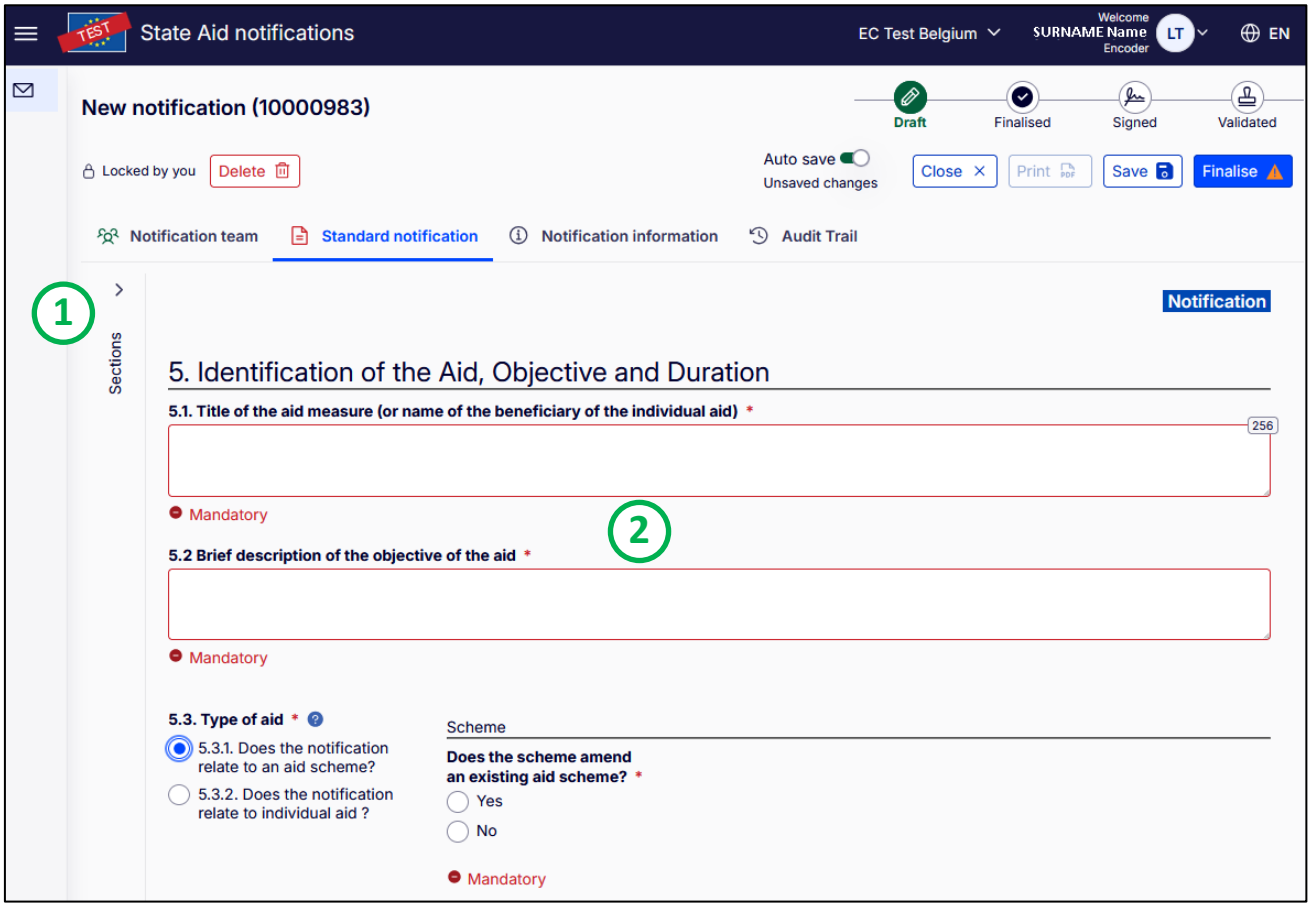


Figure 72: Collapsed form sections and mandatory fields

Make sure you answer all mandatory questions. Questions and fields left empty or containing an error, for example an invalid email address or an incorrect percentage, will result in an error message that will prevent you from finalising the notification. Error messages are always displayed below the field. All errors are also listed in the **'Validation summary'** (point 1, Figure 73).

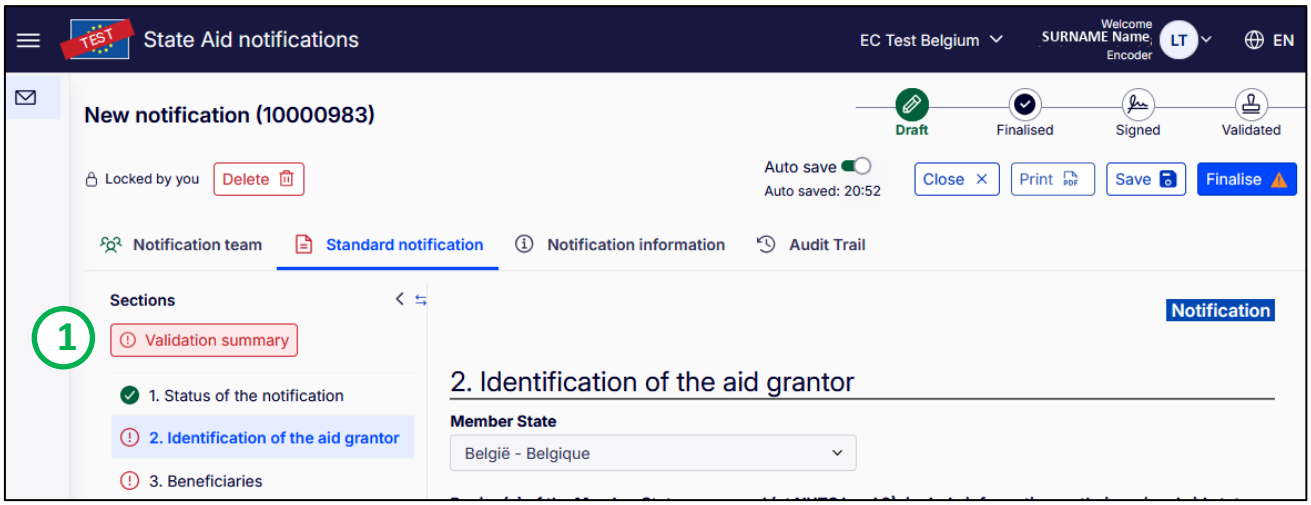


Figure 73: Validation summary button

The validation summary lists for each section in the form the elements for which an error is reported and the reason of the error (point 1, Figure 74) as well as the total number of errors in the form (point 2, Figure 74).



Figure 74: Validation summary overview

It is recommended that you follow the order of the sections in which they appear as the forms contain conditional answers which may result in a set of subsequent, related questions. If you choose an answer that requires additional information (point 1, Figure 75), additional fields will appear that need to be completed (point 2, Figure 75).

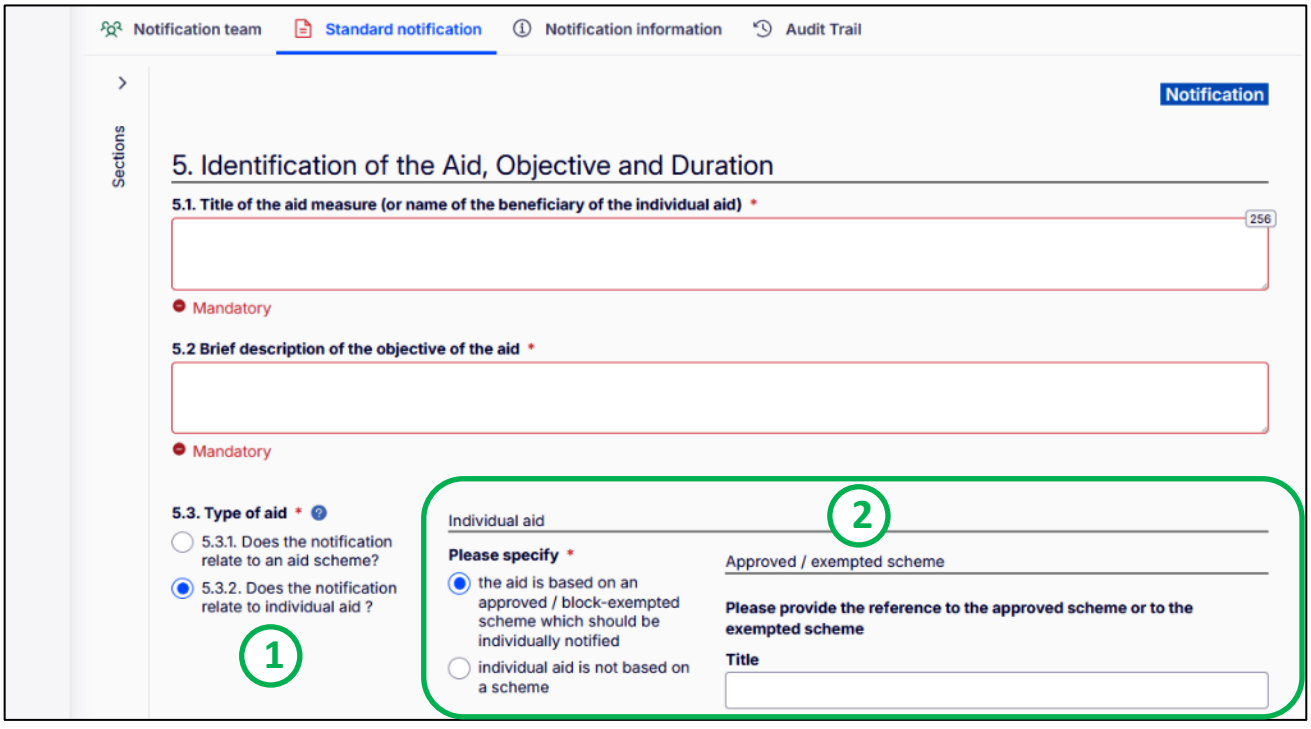


Figure 75: Conditional questions

For mandatory questions where only one option can be selected the form uses **radio buttons** (point 1, Figure 75). For multiple choice questions, the form uses **checkboxes** (point 1, Figure 76). Unlike with radio buttons, selecting one option does not clear the others. You must manually uncheck options.

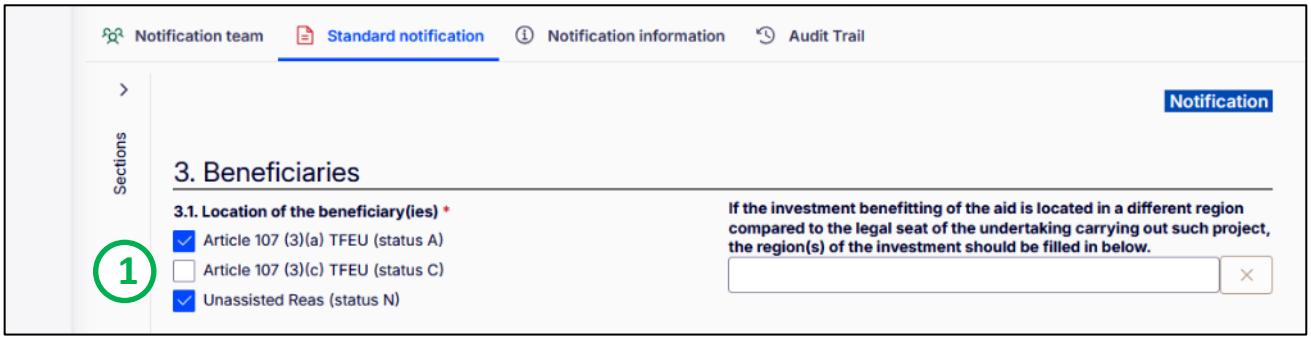


Figure 76: multiple choice questions

7.4.1. Uploading supporting documents

Each notification allows users to upload supporting documents. To upload, click on the **'Attachments**' section (point 1, Figure 77). You can upload documents either by dragging and dropping documents or a folder containing the documents, or by clicking the **'+ Add files'** or **'+ Add folder'** buttons (point 2, Figure 77).

The progress of the upload can be monitored through the progress bar (point 3, Figure 77). The system displays the upload progress for each individual document as well as the overall progress. You can navigate to other sections when the upload is in progress. The upload progress can also be monitored at the top of the notification page (point 4, Figure 77). The name and file size of each file that is selected to be uploaded are displayed in the system (point 5, Figure 77). The upload can be paused and pending uploads can be discarded (point 6, Figure 77). The status of each individual file can be consulted, the file can be renamed and each file can be individually deleted (point 7, Figure 77).

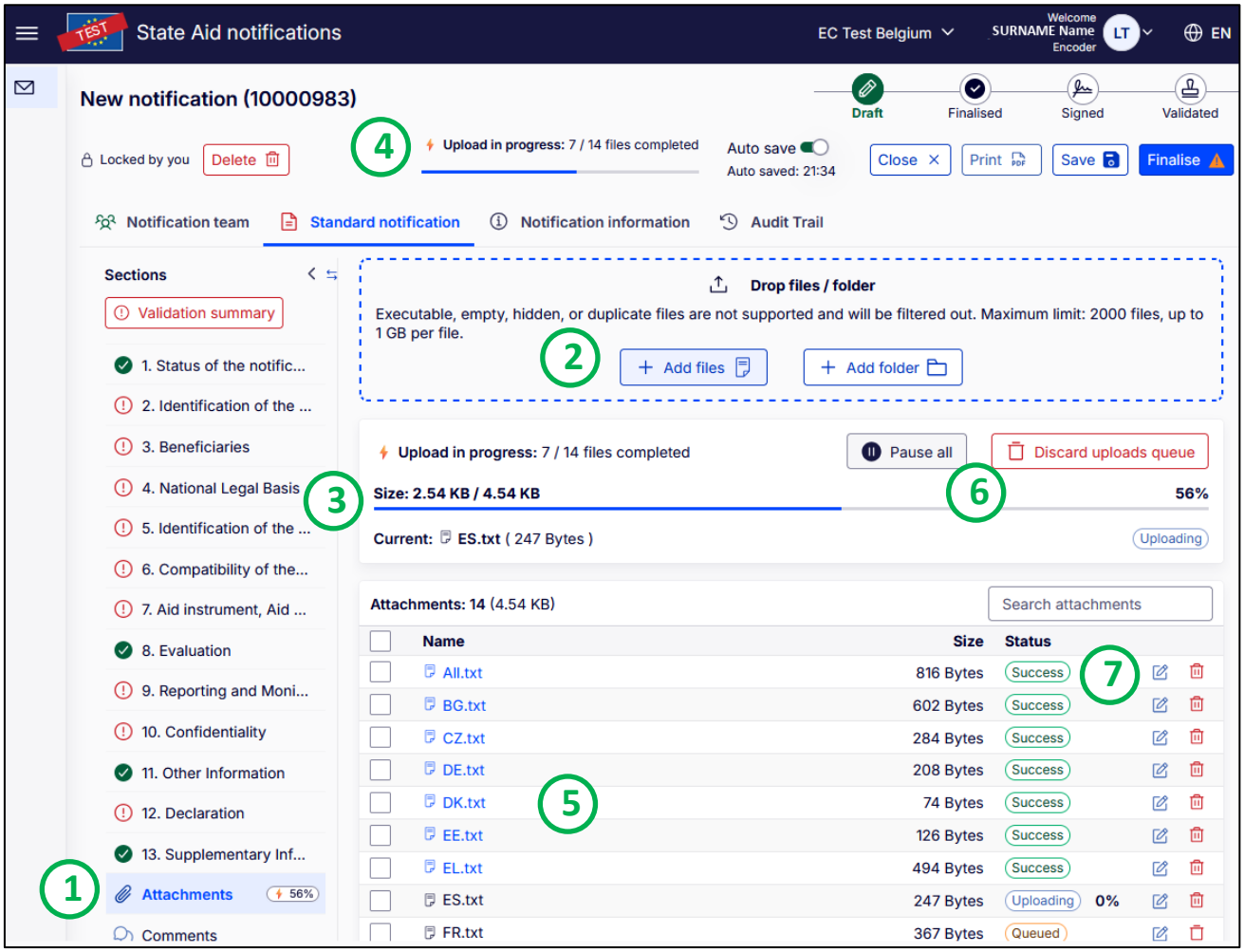


Figure 77: Upload supporting documents

7.4.2. Bulk deletion of supporting documents

To delete all uploaded documents in one go, tick the checkbox at the top of the table to select all documents (point 1, Figure 78). Click the delete button to start the deletion of the uploaded documents (point 2, Figure 78).

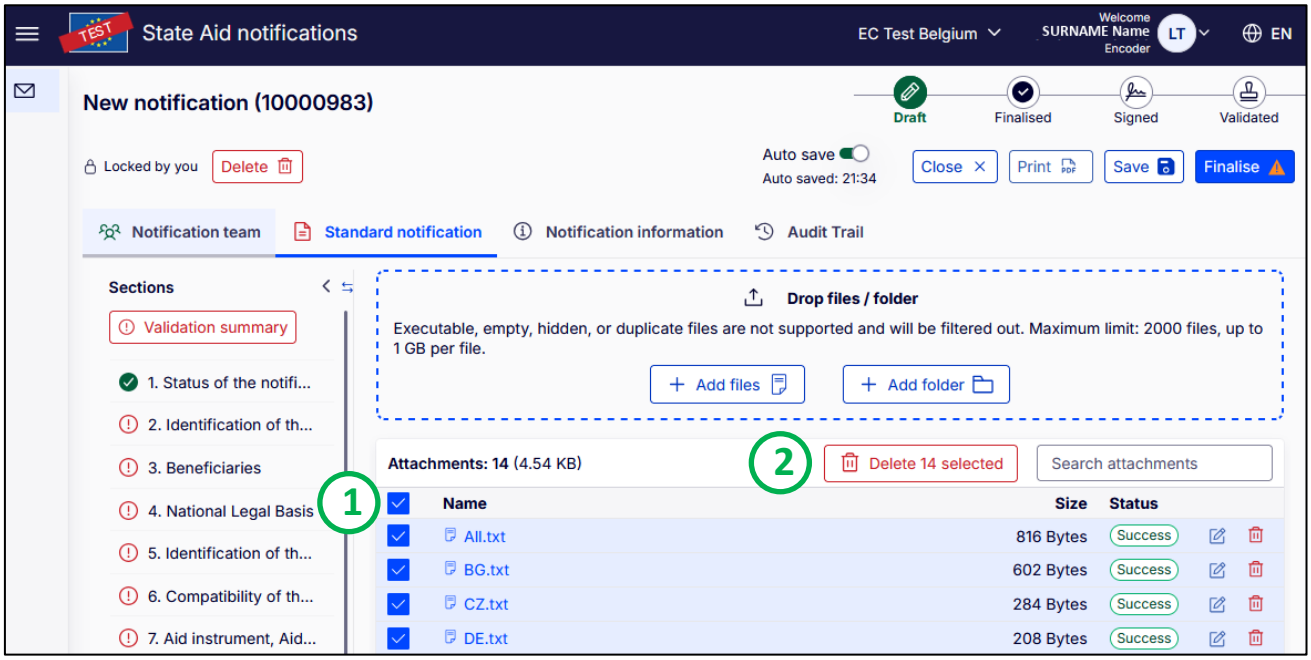


Figure 78: Bulk delete supporting documents

7.5. Notification audit trail events

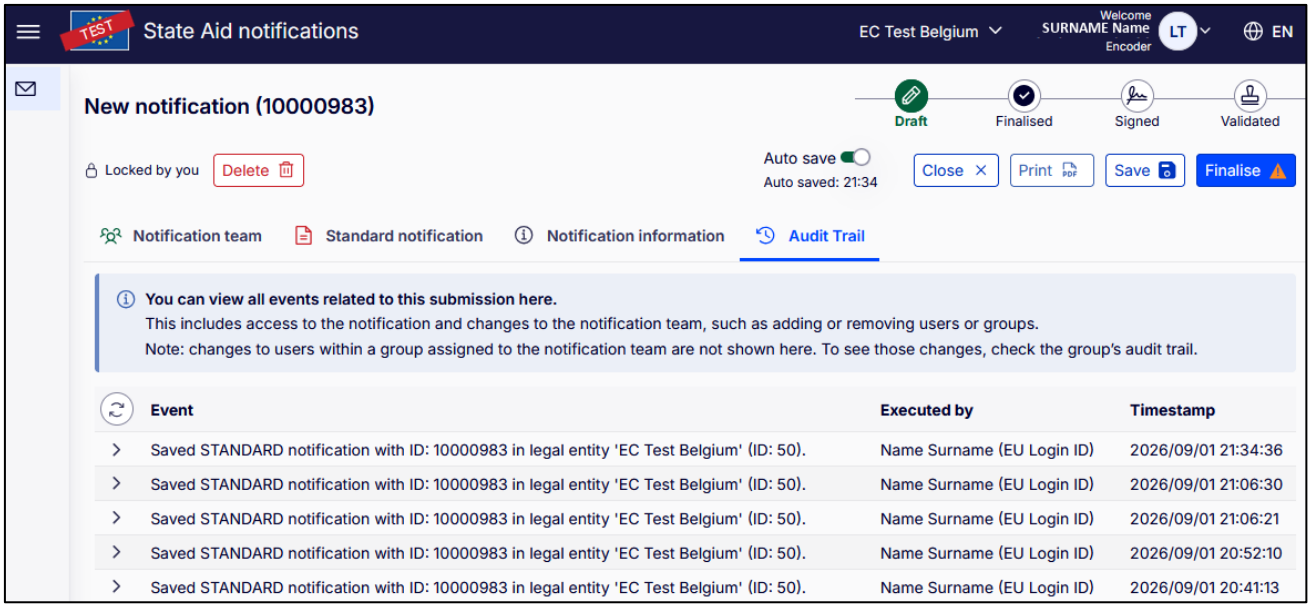


Figure 79: Notification audit trail events

At the level of each notification form, the '**Audit trail'-tab** shows the history of events related to that specific notification. It allows notification team members to view, in one place, the actions performed on the notification throughout its lifecycle.

The audit trail shows events related to:

- access to the notification;
- changes made to the notification team;
- addition or removal of individual users;
- addition or removal of groups assigned to the notification team.

This allows users to track how the notification has been handled and how access to it has evolved over time.

Important: if a group has been assigned to a notification team, the notification-level 'Audit Trail' shows the addition or removal of that group as such. However, any subsequent changes to the membership of that group (for example, if a user is later added to or removed from the group itself) are **not** displayed in the Audit Trail of the notification. To verify such changes, users must consult the Audit Trail of the relevant group.

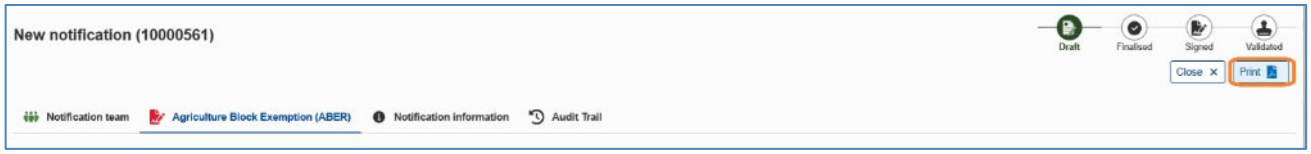
8. SPECIFIC ACTIONS ON NOTIFICATION FORMS

8.1. Print a notification

eNotifications allows users to print the content of a notification. This function is available to any team member associated with the notification as well as to Central Administrators and Local Administrators for notifications belonging to their Office(s). However, Central and Local Administrators may print a notification only if the 'Notification administrator access' setting is enabled, or if they have been added to the relevant notification team.



Click on **'Print'** icon on the right corner of the notification form.



The '**Print**' action generates a PDF version of the notification that can then be printed.

8.2. Creating a notification from a pre-notification submitted through eNotifications

If the pre-notification was submitted to the Commission through eNotifications, you can use the pre-notification to draft and submit the notification. A pre-notification team member with Encoder user rights can do so using the drop-down arrow menu in the pre-notification row. Note that this functionality is only available for pre-notifications that 1) have reached 'Validated' status, 2) have been assigned a Case number, 3) for which no notification is created yet and 4) if the Encoder is a notification team member of the pre-notification.

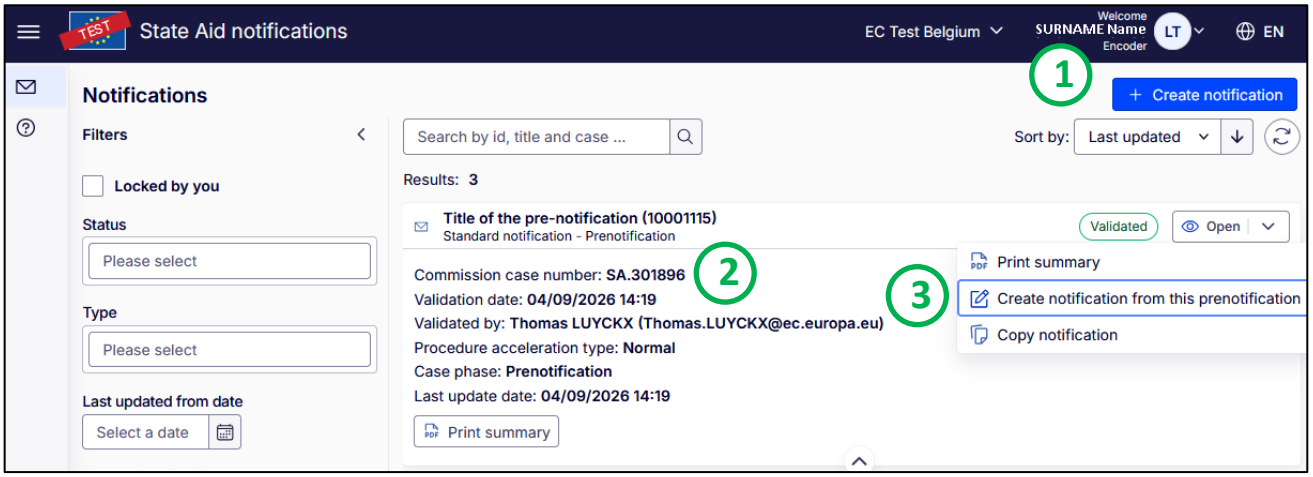
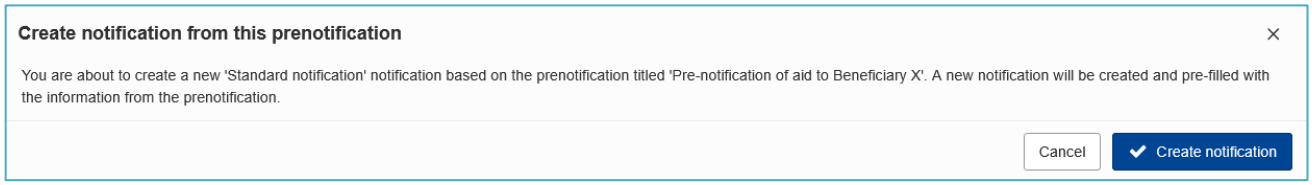
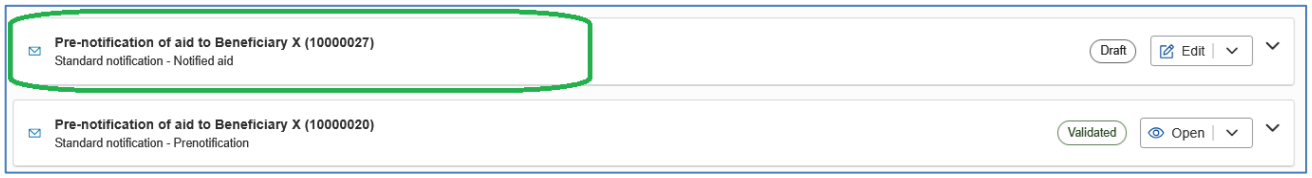


Figure 80: Create a notification from a pre-notification

The Encoder will be asked to confirm the creation of a notification.



As soon as the Encoder confirms the creation, a new notification will be available in Draft for editing with all the information from the pre-notification imported together with the notification team. Please note however that the attachments submitted in the pre-notification are **not copied** to the notification.



Since the status of the form changes from pre-notification to notification, many fields that were optional in the pre-notification become mandatory for the notification.

Any fields that were filled in during pre-notification phase can be updated, including the title of the measure.

The notification is automatically linked to the pre-notification. Thus, the SA reference is the same for both forms. Please note however that the notification must again be formally processed in eNotifications for the Commission to receive it.

8.3. Copy a Notification

eNotifications provides the option to copy notifications where suitable. This option is available only to Encoders belonging to the notification team of the notification to be copied. Notifications that were created using a previous, old version of the notification form, cannot be copied. The function is available from the notification row under the drop-down arrow menu next to **'Open'**.



Figure 81: Copy a Notification

A confirmation dialog will appear indicating the type and title of the notification being copied, for example:

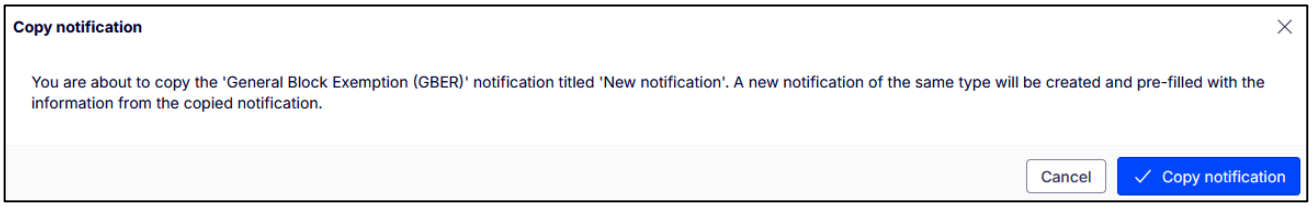


Figure 82: Example 'Copy notification' confirmation window

When copying a ‘standard notification’, the system will ask whether a ‘State Aid’ reference (Case number) has already been allocated for the new notification. For the SA reference / Case number, the same conditions and principles apply as described in section Creating a notification from a pre-notification submitted through eNotifications.

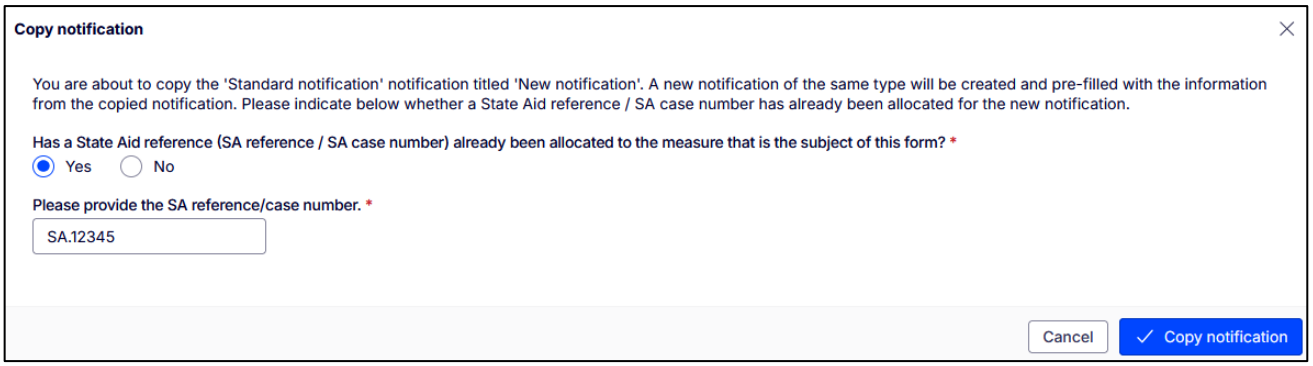


Figure 83: Example 'Copy notification' confirmation window for the standard Notification

Once confirmed, the new notification is created in ‘Draft’ status and opens for editing. The notification team is also copied automatically.

The new notification is pre-filled with the information contained in the original notification, but it can be edited as needed. The Encoder must review the copied content carefully and complete or update any mandatory fields before finalising the notification.

Attachments are not copied to the new notification and must be added again where necessary.

8.4. Deleting a Notification

Notification forms in ‘Draft’ status can be deleted. Any **Encoder** who is part of the notification team can delete a given notification. The **‘Delete’** button is available on the left-hand corner of the notification form (point 1, Figure 84).

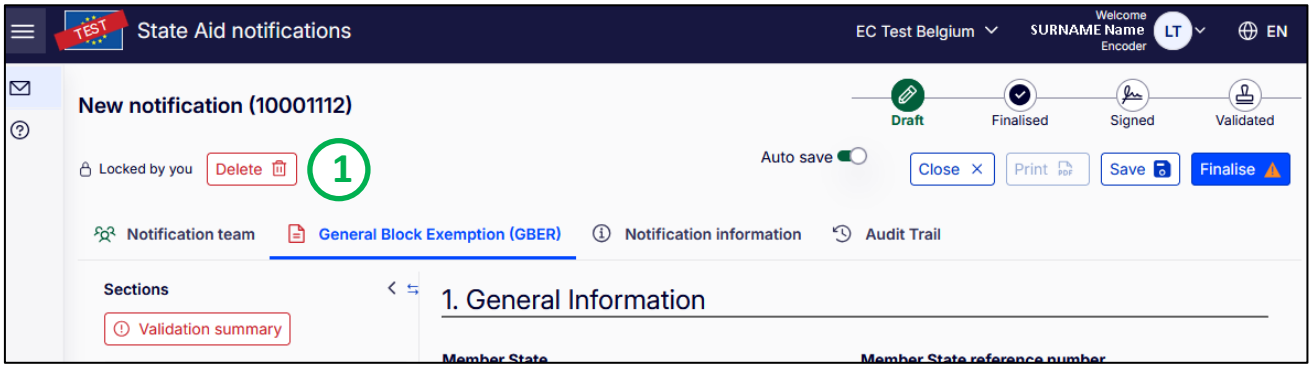


Figure 84: Delete a Notification

8.5. Withdrawing a Notification

Member States can decide to withdraw a notification. To do so, those with Validator or Central or Local Administrator profile open the relevant notification and click **'Withdraw'** (Point 1, Figure 85).

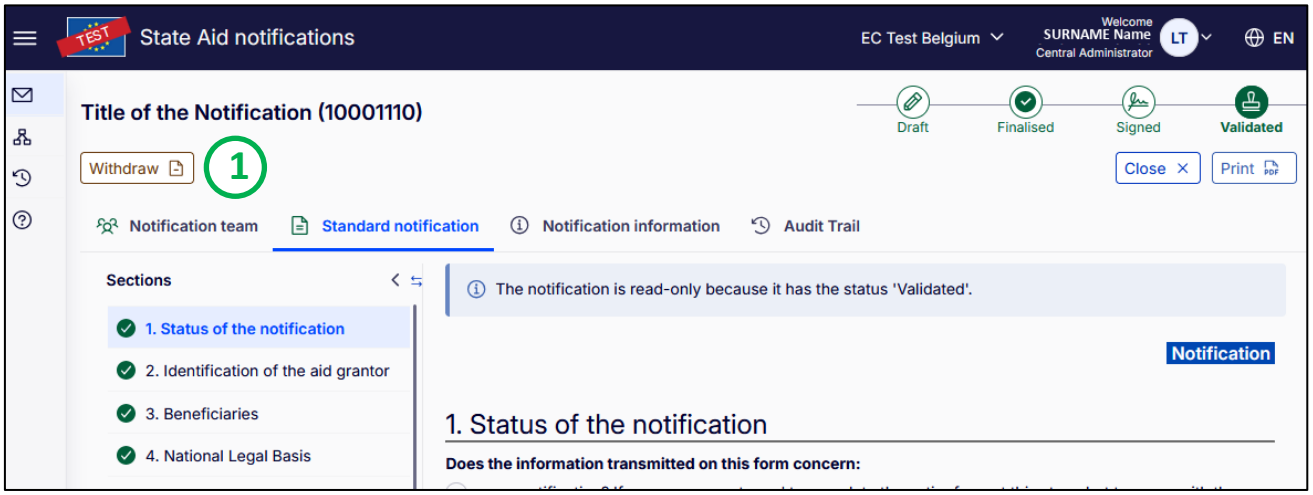
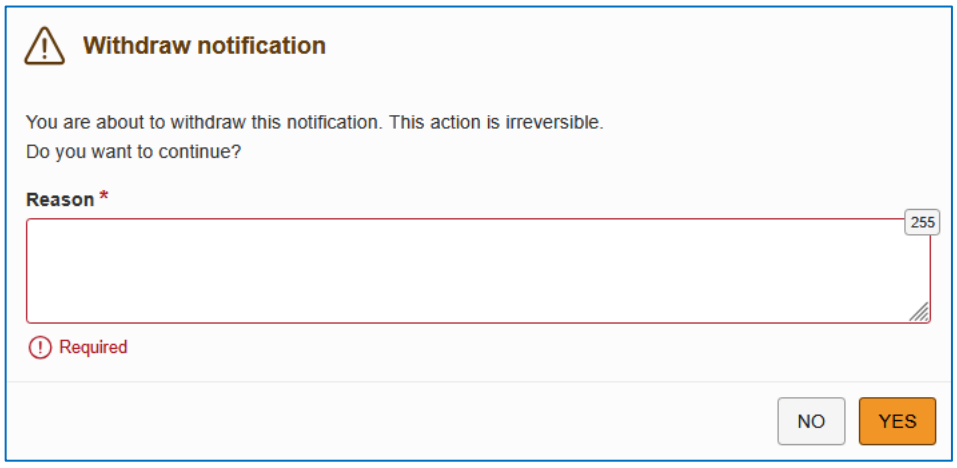


Figure 85: Withdraw a Notification

Before the withdrawal can take place, the user must provide a justification and confirm.



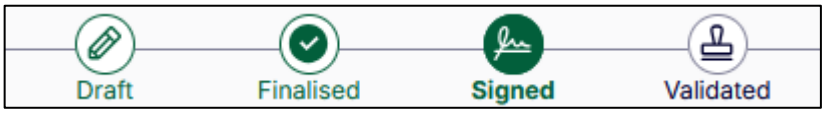
The Commission is informed that the notification has been formally withdrawn. It registers the withdrawal in its applications (including SARI2), and the notification receives the status 'Withdrawn' in eNotifications. If

block-exempted cases are involved, the information sheets published on the Commission website will be removed automatically from the website on the following working day.

9. NOTIFICATION FORMS / INFORMATION SHEETS – WORKFLOW

Any notification or summary information sheet submitted to the Commission consists of four steps, or five, in countries that include the pre-validation step for notifications.

The status bar in the upper right-hand corner shows the current status of the notification in green.



Each stage of a notification's lifecycle involves a number of profiles. The steps of 'drafting', 'finalising', 'signing' and 'validating' therefore determine who can do what and when in the notification form.

9.1. Status: 'Draft'

An Encoder can modify and update a notification as long as it is in 'DRAFT' status. For notification forms and pre-notification forms, the Encoder can also switch from pre-notification to notification and vice versa.

Once the notifications are ready for signing, Encoders finalise them.

9.2. Status: 'Finalised'

Once the notification has been finalised, it goes to the Signatory. This means that only those who have been assigned a Signatory profile in eNotifications and have been added to the notification team can update the notification.

The Signatory can also reject the notification. It then reverts to 'Draft' status. The Encoder can then make the necessary changes before submitting it again to the Signatory.

9.3. Status: 'Signed'

Once the Signatory signs the notification in eNotifications, it is considered equivalent of a handwritten signature. The notification can no longer be modified. It then goes to the Validator (or Pre-validator).

However, if changes are still needed, the Validator can reject the notification. This reverts the status to Draft, and the Encoder can then make modifications to it and resubmit it to the Signatory. The Encoder can also delete the notification if appropriate.

9.4. Status: 'Validated'

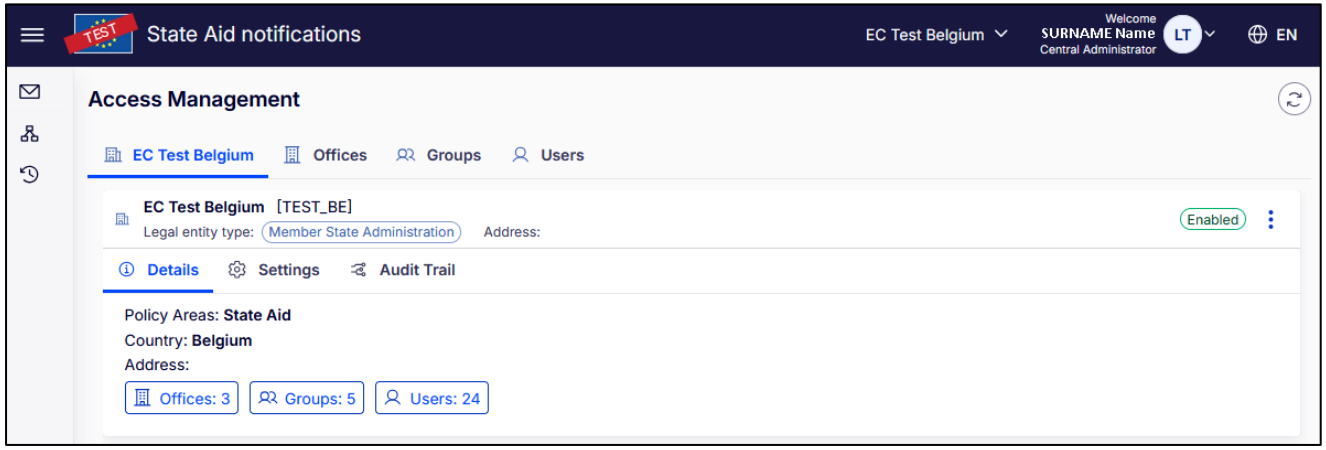
Once the Validator validates the notification in eNotifications, no further changes are possible. The notification is sent to the Commission, which registers it in its IT system and provides the Member State with the State Aid Case number under which the notification has been registered and will be handled.

Each of the formal steps in the workflow triggers an e-mail alert to inform the relevant member of the notification team that the relevant action has taken place.

10. ANNEXES

10.1. Annex 1. User Authorisation Matrix

10.1.1. Authorisation matrix for 'Access management' Module (Section 6)



10.1.1.1. ‘Access management’ Module / ‘Legal entity’ tab

	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	Own Legal Entity	Own Legal Entity					
View legal entities	✅	✅	⛔	⛔	⛔	⛔	⛔
Create legal entity	⛔	⛔	⛔	⛔	⛔	⛔	⛔
Update legal entity	✅	⛔	⛔	⛔	⛔	⛔	⛔
Enable / Disable legal entity	⛔	⛔	⛔	⛔	⛔	⛔	⛔
View legal entity settings	✅	✅	⛔	⛔	⛔	⛔	⛔
Update legal entity settings	⛔	⛔	⛔	⛔	⛔	⛔	⛔

10.1.1.2. ‘Access management module’ / ‘Offices’ tab

	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	All offices in own Legal Entity	When managing the office					
View offices	✅	✅	⛔	⛔	⛔	⛔	⛔
Create office	✅	⛔	⛔	⛔	⛔	⛔	⛔
Update office	✅	✅	⛔	⛔	⛔	⛔	⛔
Disable office	✅	✅	⛔	⛔	⛔	⛔	⛔
Delete office	✅	✅	⛔	⛔	⛔	⛔	⛔
Add user(s)	✅	✅	⛔	⛔	⛔	⛔	⛔
Remove user(s)	✅	✅	⛔	⛔	⛔	⛔	⛔

10.1.1.3. ‘Access management module’ / ‘Groups’ tab

	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	All Groups in own Legal Entity	All Groups owned by their Unit					
View groups	✅	✅	⛔	⛔	⛔	⛔	⛔
Create group	✅	✅	⛔	⛔	⛔	⛔	⛔
Update group	✅	✅	⛔	⛔	⛔	⛔	⛔
Disable group	✅	✅	⛔	⛔	⛔	⛔	⛔
Delete group	✅	✅	⛔	⛔	⛔	⛔	⛔
Add user(s)	✅	✅	⛔	⛔	⛔	⛔	⛔
Remove user(s)	✅	✅	⛔	⛔	⛔	⛔	⛔

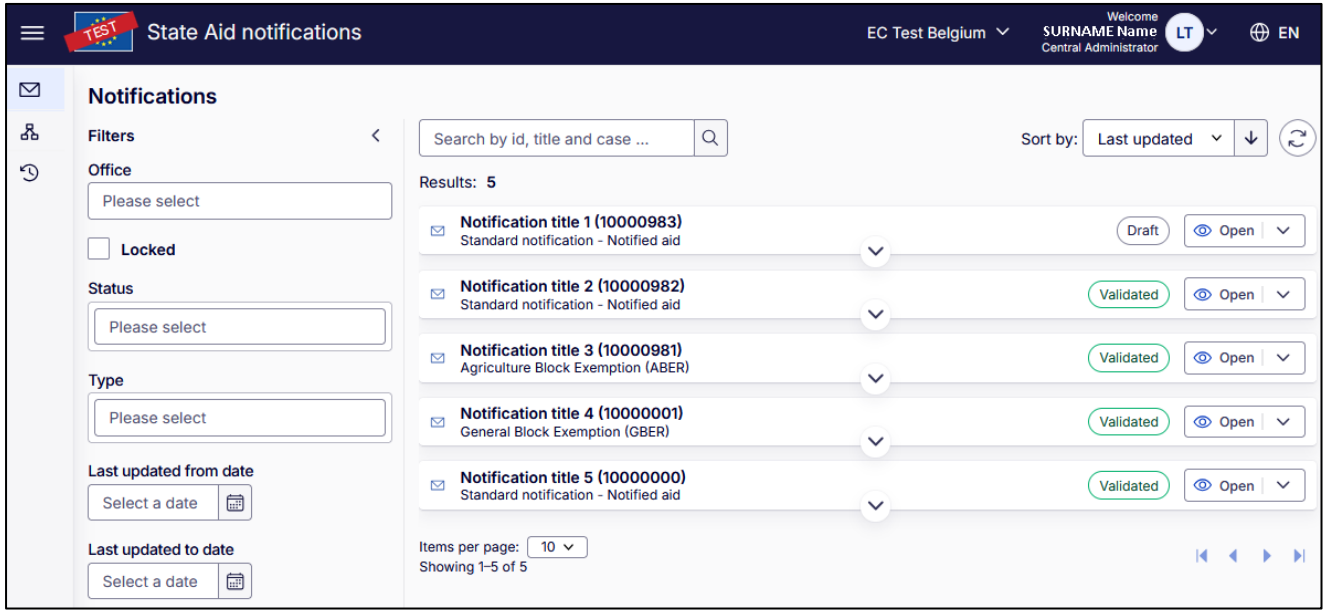
10.1.1.4. ‘Access management module’ / ‘Users’ tab

	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	All users in own Legal Entity	Users in own managed Unit(s)					
View users	✅	✅	⛔	⛔	⛔	⛔	⛔
Create user	✅ [1]	✅ [1]	⛔	⛔	⛔	⛔	⛔
Update user	✅	✅	⛔	⛔	⛔	⛔	⛔
Enable / Disable user	✅	✅	⛔	⛔	⛔	⛔	⛔
Reassign notifications	✅ [3]	✅ [3]	⛔	⛔	⛔	⛔	⛔
Resend registration invitation	✅	✅	⛔	⛔	⛔	⛔	⛔

[1] Each admin type may only assign a subset of profiles when creating a user: **Central Administrator** may assign Encoder, Signatory, Prevalidator, Validator, Viewer, Central Administrator or Local Administrator; **Local Administrator** may assign Encoder, Signatory, Prevalidator, Viewer or Local Administrator; **EC Administrator** may assign only Central Administrator or EC Administrator.

[3] Despite the name, this action does not take notifications away from the source user. They keep exactly the access they had before. When you "reassign notifications" it gives the target user the same access to the source user's notifications (the same notifications teams) in addition to what the target user already has. Use it to give a colleague access to someone's notifications, for example as a backup or when covering for them and not to move ownership away from the source user.

10.1.2. Authorisation matrix for 'Notifications' Module (section 6)



10.1.2.1. Notifications list page

Notifications list page: the page where all relevant ***Submissions*** are listed							
	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	For all notifications from own legal entity	For all notifications from own office(s)	If notification team member	If notification team member	If notification team member	If notification team member	If notification team member
View list of notifications	✅	✅	✅	✅	✅	✅	✅
Open the notification page	✅	✅	✅	✅	✅	✅	✅
Unlock a notification	✅	✅	✅	✅	✅	✅	✅
Create a notification	⛔	⛔	✅	⛔	⛔	⛔	⛔
PDF export notification meta data	✅	✅	✅	✅	✅	✅	✅

10.1.2.2. Notification page – 'Notification Team' tab

	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	For all notifications from own legal entity	For all notifications from own office	If team member	If team member	If team member	If team member	If team member
View notification team	✅	✅	✅	✅	✅	✅	✅
Search user(s)	✅	✅	✅	✅	✅	✅	⛔
Add user(s)	✅	✅	✅	✅	✅	✅	⛔
Remove user(s)	✅	✅	✅	✅	✅	✅	⛔
Search group(s)	✅	✅	✅	✅	✅	✅	⛔
Add group(s)	✅	✅	✅	✅	✅	✅	⛔
Remove group(s)	✅	✅	✅	✅	✅	✅	⛔

10.1.2.3. Notification page – 'Notification' tab

		Profile (a user can be assigned one or more profiles, each with its own set of permissions)								
		Central Administrator		**Local Administrator**		**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	**Notification status**	For all notifications from own legal entity	If notification team member	For all notifications from own office	If notification team member	If notification team member	If notification team member	If notification team member	If notification team member	If notification team member
"Notification team"-tab (view notification team)		✅	✅	✅	✅	✅	✅	✅	✅	✅
"Notification"-tab (View notification)		✅ [1]	✅	✅ [1]	✅	✅	✅	✅	✅	✅
Create notification		⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔	⛔
Delete notification	Draft	⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔	⛔
	Finalised	⛔	⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔
Reject notification	Finalised	⛔	⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔
	Signed	⛔	⛔	⛔	⛔	⛔	⛔	✅	✅	⛔
	Prevalidated	⛔	⛔	⛔	⛔	⛔	⛔	⛔	✅	⛔
Edit notification		⛔	⛔	⛔	⛔	✅	✅	⛔	⛔	⛔
Save notification		⛔	⛔	⛔	⛔	✅	✅	⛔	⛔	⛔
Finalise notification		⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔	⛔
Sign notification		⛔	⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔

Prevalidate notification		⛔	⛔	⛔	⛔	⛔	⛔	✅	⛔	⛔
Validate notification		⛔	⛔	⛔	⛔	⛔	⛔	⛔	✅	⛔
Withdraw notification		✅	⛔	✅	⛔	⛔	⛔	⛔	✅	⛔
Copy notification		⛔	⛔	⛔	⛔	✅	⛔	⛔	⛔	⛔
View comments		⛔	✅	⛔	✅	✅	✅	✅	✅	✅
Create comment		⛔	✅	⛔	✅	✅	✅	✅	✅	✅
View / download attachments		⛔	✅	⛔	✅	✅	✅	✅	✅	✅
Upload / rename / delete attachments		⛔	⛔	⛔	⛔	✅	✅	⛔	⛔	⛔

[1] Central/Local Administrator can view a notification's data outside the notification team either by being a notification team member (see the adjacent column) or, **independently of team membership**, **when the notification's Legal Entity has the "Submissions admin access" setting enabled** (Manage Legal Entities > Settings, EC Administrator only). With the setting IS disabled, a Central/Local Administrator who is not a notification team member cannot view the notification.

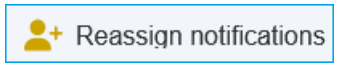
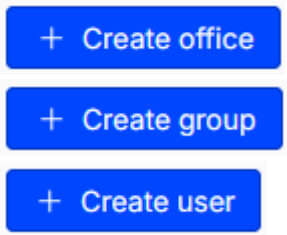
10.1.2.4. Notification page – 'Audit trail'- tab

	Profile (a user can be assigned one or more profiles, each with its own set of permissions)						
	Central Administrator	**Local Administrator**	**Encoder**	**Signatory**	**Prevalidator**	**Validator**	**Viewer**
Action	Own Legal Entity	Own managed Unit	If notification team member	If notification team member	If notification team member	If notification team member	If notification team member
View audit trail	✅	✅	✅	✅	✅	✅	✅
View audit trail entry details	✅	✅	✅	✅	✅	✅	✅

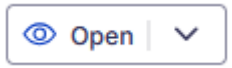
10.2. Annex 2: Overview of the buttons available in eNotifications

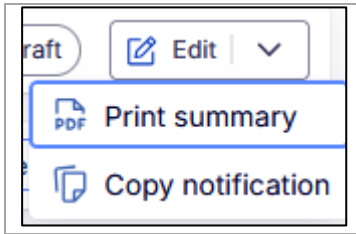
10.2.1. Buttons in Access Management Module: overview

	Description
Edit	**Edit:** allows Central Administrators and, where applicable, Local Administrators to update the properties of their legal entity, Offices, groups and users. The button is available from the three-dotted (⋮) menu on the left side of the screen. 
Disable	**Disable:** allows Central Administrators and, where applicable, Local Administrators to disable Offices, groups and users when necessary. Once disabled, these items can no longer be edited or administered in the system. Disabled users can no longer access eNotifications. This action is reversible. The button is available from the three-dotted (⋮) menu on the left side of the screen 
Enable	**Enable**: allows Central Administrators and, where applicable, Local Administrators to re-enable Offices, groups and users that are in **Disabled** status. The button is available from the three-dotted (⋮) menu on the left side of the screen. 
Delete	**Delete:** allows Central Administrators and, where applicable, Local Administrators to delete Offices and groups. Deletion is possible only if no notifications have been created within the Office or group. Deletion of users is not currently possible.

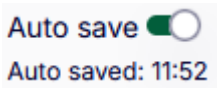
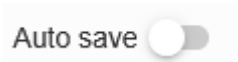
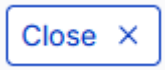
	The button is available from the three-dot vertical menu on the left side of the screen. 
	**Reassign notifications** is available only in the **Users** tab. It allows Central Administrators and, where applicable, Local Administrators to reassign notifications from one user to another. This gives the receiving user access to all notifications of the original user. The original user retains access unless their user status is Disabled. The button is available from the three-dotted (⋮) menu on the left side of the screen. 
	**+Create:** allows Central Administrators and, where applicable, Local Administrators to create new Offices, groups and users in eNotifications.

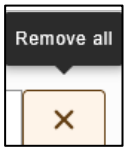
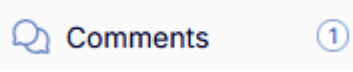
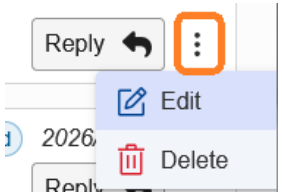
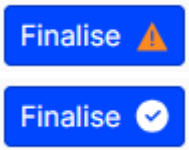
10.2.2. Buttons in Notifications Module: overview

	Description
	**+ Create notification** creates a new draft notification form. Available only to **Encoders**.
	**Edit** allows **Encoders** to open and edit notification forms in **Draft** status.
	**Open** allows notification team members to open their notification forms. Also available to **Central Administrators** and, where applicable, **Local Administrators**.
	Print summary generates a PDF containing summary information, such as the notification title and the type of form used.

	Available from the drop-down menu next to **Edit** or **Open**.

10.2.3. Buttons in Notifications forms: overview

	Description
	**Auto-save** allows to activate the auto-save mode on the notification form in Draft status. If auto-save is activated, the system automatically saves changes made to the notification form. Auto-save occurs 6 seconds after each modification introduced. Closing the notification with the 'Close' button also triggers an automatic save. Auto-save can be disabled. The system will remember the setting. 
	**Close:** closes the notification form and unlocks it for other authorised users.
	**Print:** generates a PDF version of the notification.
	**Save:** allows users to save changes made to the notification form.
	**Delete:** allows Encoders to delete the notification form. Delete is available only to Encoders and when the notification form is in Draft status.
	**+:** is made available in some sections of notification forms where several values are possible. It allows Encoders to add additional values required under the same question. Each value added using **+** can be deleted using the  button.

	**Remove all** is made available for fields where values are to be selected from the drop-down list. It allows Encoders to remove all the selected values in one click.
	**Validation summary:** it appears only if the system detected missing or incorrectly filled information. It allows users to view in a single place the list of all mandatory fields that have not been filled in or have been filled in incorrectly. It provides Encoders with the name of the field and the link to it.
	**Comments:** this section is for the notification team only and will not be transferred to DG COMP. Comments can be replied to. The author of the comment can also edit or delete it. 
	**Finalise:** is performed by Encoders. It allows Encoders to change the status of the notification from Draft to Finalised and to submit it to the Signatory.
	**Sign:** is performed by Signatories. It allows Signatories to mark the notification as signed and to submit it to Validators or where applicable, Pre-validators. It freezes the notification – no more changes are possible unless the Validator or Pre-validator rejects the notification.
	**Validate**: is performed by Validators. It allows Validators to formally notify the Commission about the state aid measure in question.
	**Reject:** can be performed by Signatories for Finalised notifications or by Validators, or pre-validator if relevant for the Signed notifications. It allows users to send notification back to Encoders for modifications or deletion.

	Reject action requires a justification to be added.

10.3. Annex 3. Key differences between SANI2 and eNotifications

This annex summarises the main operational and structural differences between the former SANI2 system and eNotifications. It is intended to help users familiar with SANI2 understand the main changes introduced by eNotifications.

(1) Organisational structure

In SANI2, a Member State is treated as an Office, and additional Offices can be created within that Office.

In eNotifications, the highest organisational level is the **Legal Entity**, representing the Member State. Offices may then be created under the Legal Entity as optional sub-entities. As a consequence, a user cannot be assigned in a way that would make them both **Central Administrator** and **Local Administrator** for an Office at the same time .

(2) Availability of the Local Administrator profile

In SANI2, the **Local Administrator** profile is available regardless of whether additional Offices have been created.

In eNotifications, the **Local Administrator** profile can be assigned only if at least one Office has been created under the Legal Entity .

(3) User access management

In SANI2, most user profiles are managed at national level, except for certain profiles such as Central Coordinators and Validators, which are managed by the Commission Administrator.

In eNotifications, **all user profiles**, including **Central Administrator** and **Validator**, are managed at national level by **Central Administrators** and, where applicable, **Local Administrators**.

(4) Profile names

Several profile names used in SANI2 have been renamed in eNotifications:

- **Central Coordinator** becomes **Central Administrator**
- **Encoding User** becomes **Encoder**

In addition, the **Restricted User** profile available in SANI2 is not available in eNotifications. Its function is covered by the **Viewer** profile.

(5) Commission user profiles

In SANI2, several Commission-side profiles exist.

In eNotifications, there is only one Commission profile: **EC Administrator**.

(6) Creating a new user

In eNotifications a Central Administrator or Local Administrator can add a new user by searching for their EU Login account using either:

- their email address, or
- their EU Login ID (if available).

This process is simpler than in SANI2.

- If the user already has an EU Login account, access can be granted immediately—no extra steps are needed.
- If the user isn't registered yet, the system will automatically send them an invitation. The user will appear as "pending" until they complete their EU Login registration.

(7) Administrator access to notifications

In SANI2, Central Coordinators and Local Administrators have access to the content of all notifications for their Member State.

In eNotifications, Administrator access to notification content is governed by a dedicated **notification administrator access setting**. When enabled, Central Administrators and Local Administrators have access to notifications and attachments within their scope even if they are not members of the notification team. This setting is enabled by default but can be disabled by the Member State. If disabled, Administrators must be added to the notification team in order to consult notification content and attachments .

(8) Validator access

In SANI2, Validators can access and validate all signed notifications of their Member States without needing to be added to a notification team.

In eNotifications, a **Validator** must be assigned to the notification team in order to act on a notification. However, Central or Local Administrators may enable **automatic assignment** of a Validator to all relevant notification teams.

(9) Audit trail

To support transparency, eNotifications introduce an explicit **Audit Trails** function both in the **Access Management Module** and at **notification level**. It records, among other things, access, changes to notification teams, and assignment changes.

(10) Mandatory setting up of a notification team

The eNotifications system introduces a new requirement that mandates the presence of all necessary profiles in the notification team before a notification can be marked as 'Finalised'. This ensures that the notification can be processed successfully through the defined steps: Draft, Finalised, Signed, and Validated (or five steps in countries with a pre-validation stage).

(11) Creation of new notifications

In SANI2, users with the Encoding User or Signatory profile can create notifications.

In eNotifications, only users with the **Encoder** profile can create a new notification, and they must be logged in with that profile when doing so.

(12) Handling of attachments

In SANI2, attachments are added one file at a time.

In eNotifications, attachments can be added by:

- drag and drop,
- selecting **+ Add files**, or
- selecting **+ Add folder**.

Attachments can also be renamed, deleted individually, or deleted in bulk.

(13) Copying a notification

eNotifications provides the option to copy notifications where suitable. Unlike in SANI2, a notification in eNotifications does not need to be in 'Validated' status to be copied: it can be copied regardless of its current status. This option is available only to Encoders belonging to the notification team of the notification to be copied. The function is available from the notification row under the drop-down arrow menu next to 'Open'.

(14) Creating a notification from a pre-notification

eNotifications includes a dedicated function allowing an Encoder to create a notification directly from a pre-notification submitted in eNotifications. The new notification is created in Draft status, the information is imported, and the notification team is copied. Attachments are not copied and must be added again where necessary. The notification created using this function automatically receives the same State aid number as the pre-notification.

(15) Linking to an existing DG COMP case

In eNotifications, when creating certain types of notification forms, users may indicate an existing **State aid reference (SA number)**. This allows the form to be linked to an existing case and ensures that the notification is registered by the Commission under the same SA reference, provided that the number exists and belongs to the Member State concerned.

(16) Automatic saving

eNotifications includes an **auto-save** function for Encoders for notifications in Draft status. When auto-save is activated, the system automatically saves changes 6 seconds after each modification. The system also automatically saves the notification when the notification form is closed.

(17) Workflow after Validator rejection

When a Validator rejects a signed notification in SANI2, the notification is returned to the Signatory. The Signatory must then reject it again before it is sent back to the Encoding User.

In eNotifications, when a Validator rejects a signed notification, the notification is returned directly to Draft status. The Encoder can then modify and resubmit the notification or delete it if appropriate.