

ECB Identity Portal

Procedures for Delegated User and Delegated Access

Administrators

January 2024

Authors: Alessandro Barbieri, Federica Di Marco, Laurence Langlois and Raphael Overbeck

Contents

- 1. Definition 3**
- 1.1. Assistance 4
- 2. Purpose 4**
- 2.1. Target audience 4
- 2.2. Scope 4
- 2.3. Roles and responsibilities 4
- 3. Account types..... 4**
- 3.1. Individual accounts..... 4
- 3.2. Delegated User Administrator..... 4
- 3.3. Delegated Access Administrator 5
- 3.4. Account de-activation or deletion 6
- 4. Prerequisites – creating DUAs and DAAs 6**
- 5. Login and password management 7**
- 5.1. First login, confirmation of consent and user data..... 7
- 5.2. Account login 9
- 5.3. Two-factor authentication..... 10
- 5.3.1. Second factor options 10
- 5.3.2. Setting up a default two-factor authentication 11
- 5.4. Account login failure..... 11
- 5.5. Account login success – My Apps page 12
- 5.6. Password management 13
- 5.6.1. Changing a password 13
- 5.6.2. Resetting a password 14
- 5.6.3. Password expiry 17
- 5.7. Changing a phone number 18
- 5.8. Self-deleting an account 19
- 5.9. Verifying personal information..... 20
- 6. Delegated User Administrator tasks 20**
- 6.1. Onboarding and creating a new user 20
- 6.2. Editing a user’s details 22
- 6.3. Suspending an account..... 23
- 6.4. Deleting a user..... 24
- 6.5. Granting a DUA role..... 25
- 6.6. Revoking a DUA role 26
- 7. Delegated Access Administrator – specific tasks..... 27**
- 7.1. Confirming user group membership 27
- 7.2. Adding a user to a user group (membership)..... 29
- 7.3. Deleting a user from a group..... 31
- 7.4. Granting a DAA role..... 31
- 7.5. Revoking a DAA role 33

Annex 1 – FAQs and automated responses..... 36
 Frequently Asked Questions 36
 Automated processes – screenshots 37

Glossary

Terms	Definition
iWelcome /OneWelcome	Identity as a Service forming the basis of the ECB Identity Portal.
iWelcome User Interface (iWelcome UI)	Application within the ECB Identity Portal for managing users and access rights.
Delegated Access Administrator (DAA)	An authenticated and authorised natural person who, on behalf of a third party, can assign role-specific application access rights to third-party users created by the Delegated User Administrator specific to that role.
Delegated User Administrator (DUA)	An authenticated and authorised natural person who, on behalf of a third party, manages the users within their own organisation who access ECB applications, such as ASTRA, IMAS or STAR, through their respective portals. The role is displayed on iWelcome screens as Application Access Administrator.
IDaaS	Identity as a Service.
Organisation	A legal entity that is not an individual.
Third party	A legal person who interacts with the ECB and is not acting on the ECB’s behalf.
User	In this document, a user is an authenticated and authorised natural person who, on behalf of a third party, has access to the ECB Identity Portal. Users are assigned access rights in accordance with their role.

1. Definition

The **ECB Identity Portal** is the online platform for the central identification, authentication and account management of third-party users accessing European Central Bank (ECB) internet-based portals, such as ASTRA, IMAS or STAR, that provide access to ECB applications.

User accounts are managed by:

- ECB staff, who initially set up an organisation’s Delegated User Administrator account or invite individual users from outside organisations to activate an account;
- third-party Delegated User Administrators and Delegated Access Administrators nominated by a third party and confirmed by ECB staff.

The roles and responsibilities of users are detailed in the **Terms of use for end users** and **Terms of use – supplement for Delegated User and Access Administrators**.

1.1. Assistance

For assistance, please contact the ECB Support Centre by email at servicecentre@ecb.europa.eu or by phone on +49 69 1344 7766.

2. Purpose

This document describes the procedures and processes applicable to third-party users of the ECB Identity Portal (id.ecb.europa.eu) when accessing ECB information. The ECB Identity Portal provides self-service-oriented service solution for identity and access management for all external users of a defined set of ECB services.

Some capabilities are available to all users, whereas others are available only to Delegated User Administrators and Delegated Access Administrators.

If you have any questions, please contact the ECB Support Centre by email at servicecentre@ecb.europa.eu or by phone on +49 69 1344 7766.

2.1. Target audience

This document is intended for Delegated User Administrators; Delegated Access Administrators.

2.2. Scope

The document covers the procedures performed by third-party users administering or accessing the ECB Identity Portal to manage user accounts and their group memberships.

2.3. Roles and responsibilities

The roles and responsibilities of ECB Identity Portal are set out in the Terms of use for end users and Terms of use – supplement for Delegated Users and Access Administrators, both available on the [ECB's website](#).

3. Account types

There are three types of user account on the ECB Identity Portal: Individual; Delegated User Administrator; Delegated Access Administrator.

3.1. Individual accounts

This is the default account for all users. Users can log in to the ECB Identity Portal to access other ECB portals or to manage their authentication settings.

Delegated User Administrators are able to create and manage individual accounts for users within their organisation.

3.2. Delegated User Administrator

All non-ECB organisations must have at least two Delegated User Administrators (DUAs) who are independent of the ECB application for which they administer access. An organisation without the requisite number of DUAs will be deleted from the system and all users within that organisation will cease to have access to the ECB Identity Portal and ECB applications.

When creating new third-party users from their own organisation, DUAs:

- i. must use their own organisation's email domain (note that an organisation may have multiple domains) as per the [Terms of use – supplement for Delegated User and Access Administrators](#), for example: firstname.lastname@banque-xyz.abc;

- ii. must not use public accounts, such as Yahoo, Hotmail or Gmail.

DUAs are specifically responsible for:

- i. creating users (and actively responding to user creation requests initiated through underlying ECB applications);
- ii. granting and revoking DUA roles within the organisation;
- iii. providing local user support, e.g. by maintaining user data;
- iv. actively participating in the reconciliation and recertification of third-party user-management users by ensuring identity data are complete and up to date;
- v. regularly reviewing user data to ensure that they are up to date;
- vi. being entirely familiar with codes for subsidiaries (misspelling may cause access issues).

DUAs must:

- i. inform the ECB of local incidents related to user management;
- ii. deactivate the accounts of users who leave an organisation and notify the ECB accordingly without undue delay (the ECB is not liable if a DUA fails to do so).

DUAs must inform all Delegated Access Administrators in their organisation of any changes in the role or responsibilities of a user within their organisation (the ECB is not liable if a DUA fails to do so).

3.3. Delegated Access Administrator

ECB staff can assign Delegated Access Administrator (DAA) status on receipt of an approved request (see below).

DAAs are responsible for:

- i. implementing access to a defined set of ECB services in line with their organisation’s need-to-know requirements;
- ii. granting and revoking DAA roles for the application(s) under their responsibility;
- iii. adding local users to groups under the responsibility of their organisation’s DAAs;
- iv. removing local users from groups under the responsibility of their organisation’s DAAs;
- v. providing support to local users, e.g. by assigning appropriate access rights and solving access rights issues;
- vi. conducting an annual review of group memberships and regular recertification to ensure user access is up to date;
- vii. informing the ECB of local incidents related to group management.

Table 1: Roles and permissions matrix | User roles

	DUAs	DAAs
Users		
View users	X	X
Edit users	X	
Create users	X	
Delete users	X	

Grant and revoke DUA roles	x	
Grant and revoke DAA roles		x
Add and remove group memberships (within the scope of the application concerned)		x

3.4. Account deactivation or deletion

Third-party users are required to follow ECB guidance as regards user data, account security and user behaviour. The ECB may deactivate or terminate user accounts without prior notice if users fail to follow this guidance or if it detects:

- i. abusive behaviour;
- ii. account hacks;
- iii. data leaks.

User accounts will also be deactivated or deleted if:

- i. an account remains unused for six months – where this is the case, the ECB will send a notification to the user and will delete the account if there is no response within six months;
- ii. a user has changed roles or has left the organisation – in this instance, DUAs are expected to have processes in place to delete such users.

4. Prerequisites – creating DUAs and DAAs

An organisation wishing to access the ECB Identity Portal first needs to appoint at least two DUAs. At the request of an ECB counterpart, an ECB approver issues an invitation to a user to provide the following information in order to create an account:

- i. first name;
- ii. last name;
- iii. phone number (including the country code, e.g. +49 for Germany or +353 for Ireland);
- iv. email address (linked to the user’s official organisation, e.g. a bank or academic institute, as per the Terms of use for end users of the ECB Identity Portal);
- v. official organisation;
- vi. expiration date (if the account is temporary).

Once users have provided this information and given active consent for their data to be stored on ECB systems by agreeing to the ECB’s [Privacy statement for the ECB Identity Portal](#), the account is created. Active users of the ECB Identity Portal may be promoted to DUAs or DAAs by existing Delegated Administrators.

5. Login and password management

There are two ways for users to log in to ECB portals:

- i. The user accesses the ECB application and is redirected to the ECB Identity Portal.
- ii. The ECB Identity Portal authenticates the user.
- iii. The user is redirected to ECB third-party application.

Or

- i. The ECB Identity Portal authenticates the user.
- ii. The user accesses the My Apps page.
- iii. The user then accesses ECB third-party applications directly.

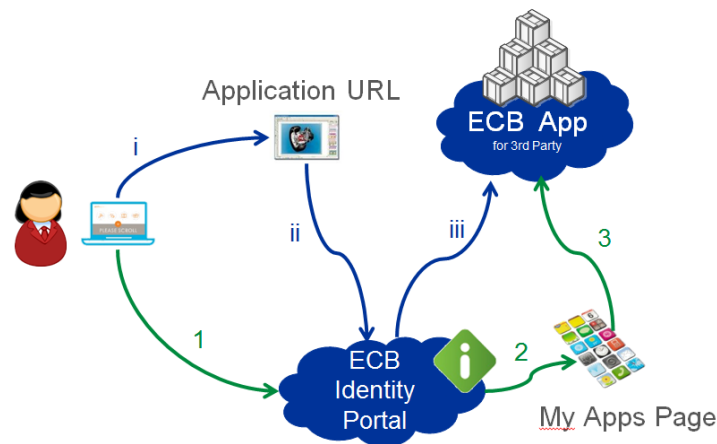


Figure 1: How a user can log in to an ECB application.

5.1. First login, confirmation of consent and user data

Users receive an email and can log in for the first time using the link in that email and a confirmation code sent by text or voice message.



Before setting a password, users will be asked to confirm their consent to the ECB’s privacy policy and to the Terms of use for end users of the ECB Identity Portal:

EUROPEAN CENTRAL BANK | EUROSISTEM
ECB Identity Portal

Set your password

New password

- use at least 10 characters

Use at least 3 of the following categories:

- use at least 1 uppercase letter (ABC...)
- use at least 1 lowercase letter (abc...)
- use at least 1 number (12345...)
- use at least 1 special character (!@#\$%^&*)

Confirm password

- passwords match

Consent

- I agree with the [Privacy Policy](#)
- I agree with the [Terms of Service](#)

If the user does not agree, they can ask for their account to be deleted by contacting the ECB Support Centre. (See the question “I am experiencing issues with my account. Who can I contact for more support?” in the Frequently Asked Questions (FAQs) displayed on screen and in Annex 1 below.).

The ECB will ask the user to reconfirm their consent at regular intervals and when there are changes to the terms of use for end users of the ECB Identity Portal.

5.2. Account login

To access ECB portals, users must log in using a two-factor authentication method through the [ECB Identity Portal](#). The first authentication factor is a correct username, in this case a user’s email address, and a password. Users should enter their registered email address in the **Email Address** box, put in their password and click **Log in**.

The **Login from ECB network** option is only for users who are connected to the ECB network and have an @ecb.europa.eu email address. Standard credentials for the ECB network should be used if they are requested after clicking the link.

5.3. Two-factor authentication

For third-party users, the second authentication factor is a code provided by text voice message, QR code or push notification.

5.3.1. Second factor options

After logging in to <https://id.ecb.europa.eu> with their email address and password, users must obtain the second authentication factor – a security code sent by:

- a. text message;
- b. voice message;
- c. QR code;
- d. push notification.

Note: The default setting is for a text message. If users wish to change the default method, they will have to restart the login process. The QR code and push notification methods are only available once the OneWelcome Authenticator mobile app is downloaded and linked to the user account.

Users must select their preferred two-factor authentication method.

EUROPEAN CENTRAL BANK | EUROSISTEM
ECB Identity Portal

Secure login

A verification code is sent to this phone number:
+4xxxxxxxx737

Please enter the code you received *

[Resend code using SMS](#)

[Resend code using Voice](#)

Other
 Login

EUROPEAN CENTRAL BANK | EUROSISTEM
ECB Identity Portal

Secure login

Select a secure login option

Send an SMS code

Send a voice message

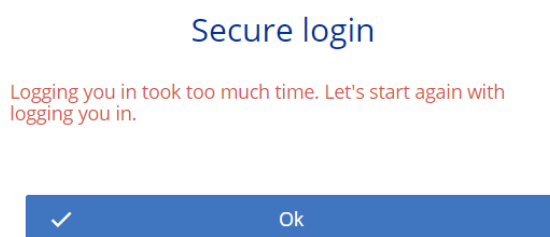
Send a push notification

Scan QR code

- a. Users receive the security code by text message sent to a mobile phone and must then enter that code on the **Secure login** page.
- b. Users receive the code by voice message and must then enter that code on the **Secure login** page.
- c. Users log in to the OneWelcome Authenticator mobile application, then click the **Scan QR code on website** button on the homepage and scan the QR code on the website login page.
- d. Users log in to the OneWelcome Authenticator mobile application to accept the push notification on the homepage.

If a user receives a notification but was not attempting to log in at that time, they should answer “No, it is not me” and report this to their DAA or to the ECB Support Centre.

If the secure login times out, e.g. because logging in took too long or the security code was not received, the following panel will appear.



5.3.2. Setting up a default two-factor authentication

Once logged in, users can change the way in which they receive the second authentication factor. Once a new preference is selected, this becomes the default method for that user. Consequently, if a user selects **by voice**, this setting is stored and voice message will be selected by default the next time the user logs in and will remain the default setting thereafter.

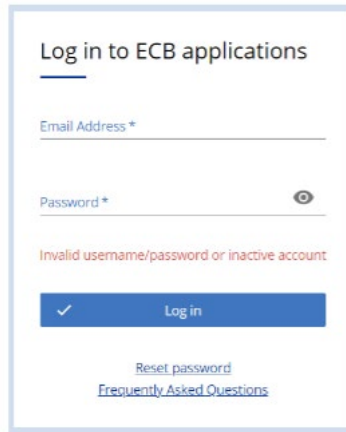
The security code contains six numbers. To make the code easier to understand, the voice message starts a few seconds after the user answers the call. The voice message says:

“Your security code is [security code, number by number]. I repeat, your security code is [security code, number by number].”

- a. The link **Resend code using voice** sends a new code, with the same message format. Only the most recent code is valid.
- b. The code must be entered within three minutes of the password. If this time is exceeded, users will have to re-enter their email and password and request a new code.

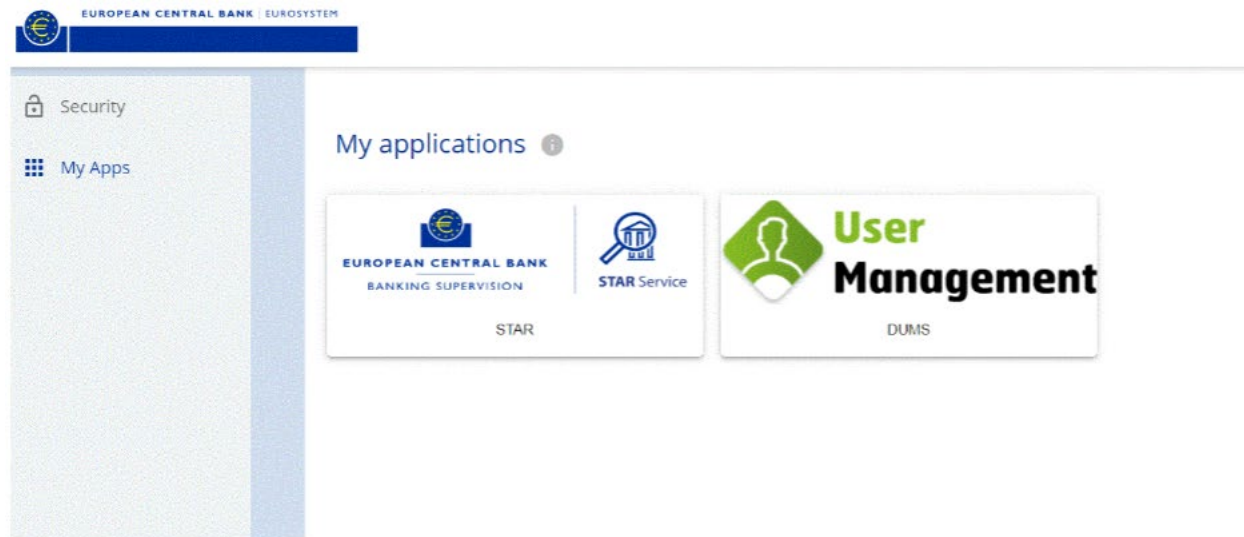
5.4. Account login failure

If a user enters incorrect login details, the following error message will be displayed. The user can then attempt to log in again.



5.5. Account login success - My Apps page

Once they have logged in, users will be taken to a landing page similar to the one below. They can then select one of the available applications.



5.6. Password management

5.6.1. Changing a password

Once logged in, users can change their password on the **Security** page.

The screenshot shows the ECB Identity Portal interface. At the top, there is a navigation bar with the ECB logo and the text 'EUROPEAN CENTRAL BANK | EUROSYSTEM' and 'ECB Identity Portal'. A red arrow points to a hamburger menu icon on the left. Below the menu, a dropdown menu is open, with the 'Security' option highlighted by a red box. The 'Security' page contains a 'Change password' section with the following elements:

- 'Current password' text label above a text input field with a toggle icon.
- 'New password' text label above a text input field with a toggle icon.
- A list of password requirements, each with a checked checkbox:
 - use at least 10 characters
 - Use at least 3 of the following categories:
 - use at least 1 uppercase letter (ABC...)
 - use at least 1 lowercase letter (abc...)
 - use at least 1 number (12345...)
 - use at least 1 special character (!@#\$%^&*)
- 'Confirm new password' text label above a text input field with a toggle icon.
- A checked checkbox labeled 'passwords match'.
- A grey button with a checkmark icon and the text 'Change password'.

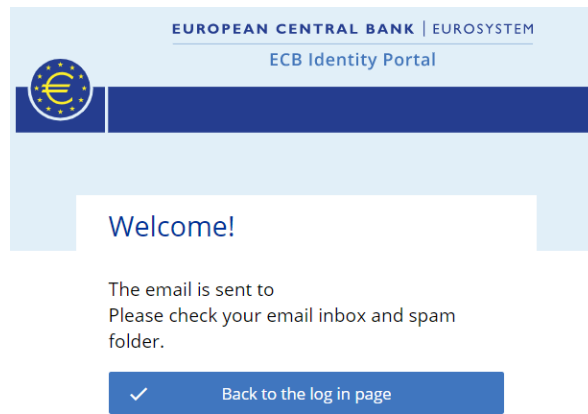
Users must enter their current password, their new password, checking that it meets the password requirements stated on the page, and then confirm their new password.

5.6.2. Resetting a password

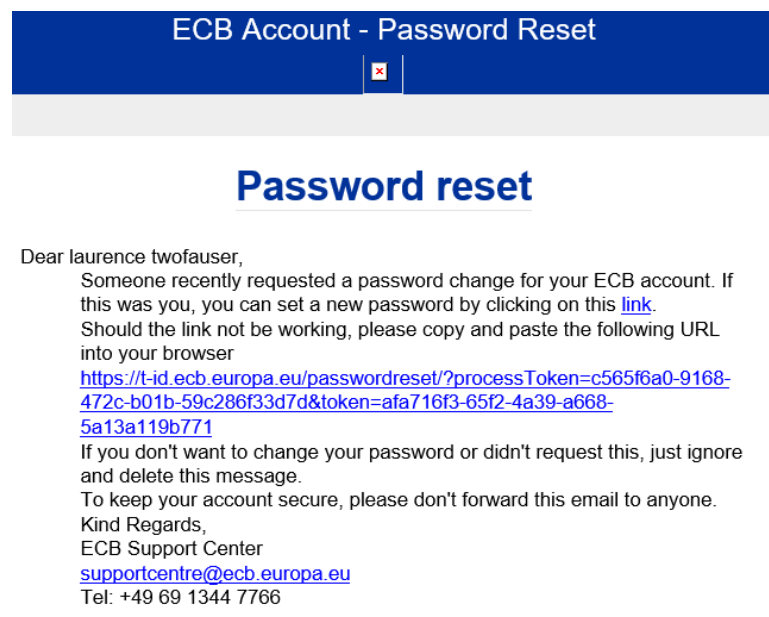
Users can reset their password by clicking **Activate or reset password** on the login page or by visiting the help page containing the [Frequently Asked Questions](#) (see [Annex 1](#)).

[Login from ECB network](#) | [Privacy statement](#)

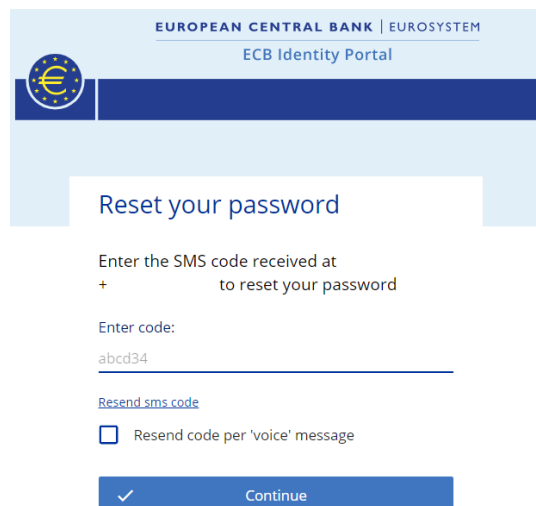
- a. The user must click **Activate or reset password**.
- b. The user must enter their email address and click **Continue**.



c. The user will receive the following email.



- d. The link takes the user to the **Reset your password** page to enter the second authentication factor.
- e. The user is prompted to enter the security code received by text or voice message and then clicks **Continue**.



f. The user can then enter a new password that meets the password requirements.

EUROPEAN CENTRAL BANK | EUROSYSTEM
ECB Identity Portal

Password reset

New password

- use at least 10 characters
- Use at least 3 of the following categories:
- use at least 1 uppercase letter (ABC...)
- use at least 1 lowercase letter (abc...)
- use at least 1 number (12345...)
- use at least 1 special character (!@#\$\$%^&*)

Confirm password

- passwords match

g. The user is asked if they want to **Log out from all devices**. To avoid future password confusion, the user should log out from all devices by clicking **Yes**.

EUROPEAN CENTRAL BANK | EUROSYSTEM
ECB Identity Portal

Logout from all devices?

Would you like to logout from all devices?

- h. After successfully resetting their password, the user will receive the following automated confirmation email. \$\$

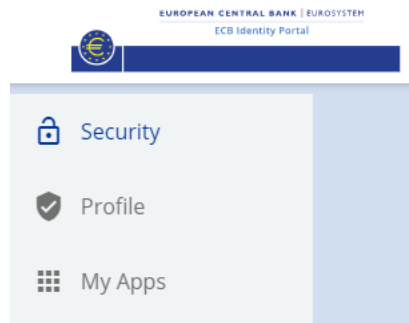


5.6.3. Password expiry

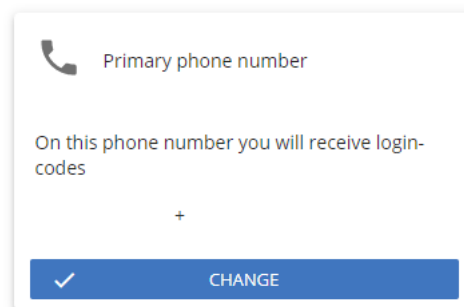
In the event of non-activity, the password will expire 180 days after the last login.

5.7. Changing a phone number

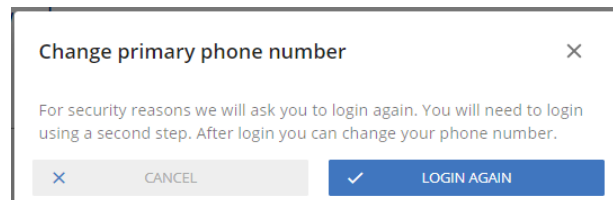
Once logged in, users can change their phone number on the **Security** page.



Change Phone Number

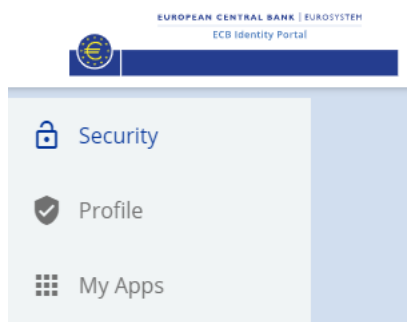


- a. The user should click **CHANGE**.
- b. The user then changes the number and is asked to log in again to confirm the change.

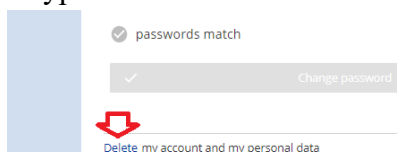


5.8. Self-deleting an account

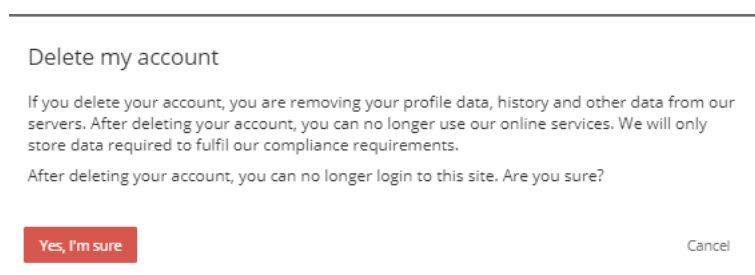
Once logged in, users can delete their own account and personal data on the **Security** page.



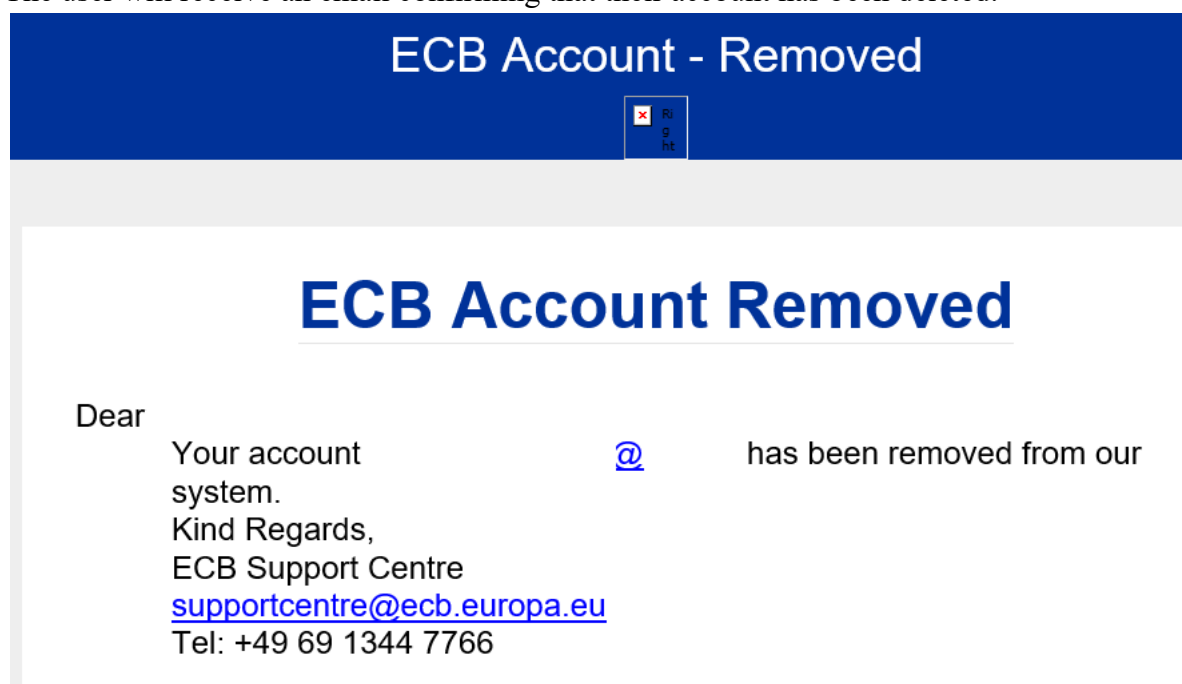
- a. The user should click the **Delete** hyperlink at the bottom of the page.



- b. The user must then confirm deleting their account by clicking **Yes, I'm sure**.



- c. The user will receive an email confirming that their account has been deleted.



5.9. Verifying personal information

Users can check the information included in their profile. If any data are incorrect, the user should contact the party that created the user account and ask for the data to be corrected.

The screenshot displays the 'My personal info' page in the ECB Identity Portal. On the left, a sidebar contains navigation options: 'Security', 'Profile', and 'My Apps'. The main content area is titled 'My personal info' and includes the following fields:

- Name ***: A text input field.
- Surname ***: A text input field.
- Email**: A section header with an information icon. Below it, there is a sub-section for 'Email address' with a 'Work' label and a 'My primary email address' label.
- Phone**: A section header with an information icon. Below it, there is a sub-section for 'Phone number' with a 'Work' label and a 'My primary phone number' label.

The footer of the page contains the text 'Copyright 2021, European Central Bank' and links for 'Login for ECB users' and 'Privacy Policy'.

6. Delegated User Administrator tasks

User management is a core part of an organisation's directory services and provides basic security. It enables administrators to control the access of users, both onboard and offboard, to and from an organisation's various IT systems and resources. A directory service will then authenticate, authorise and audit user access to those IT resources based on the rules set by the IT administrators.

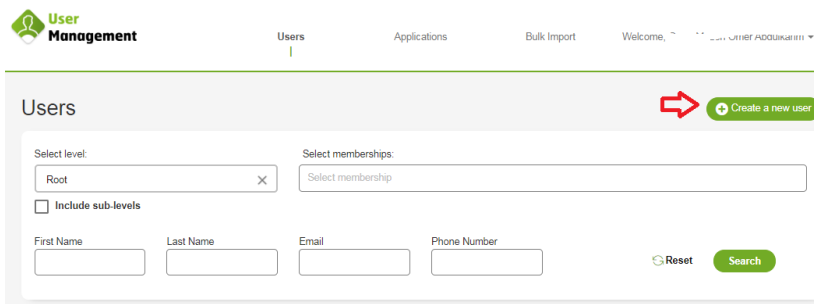
6.1. Onboarding and creating a new user

A new user will receive a welcome email containing instructions on the software and applications that they will need to access. The user must have:

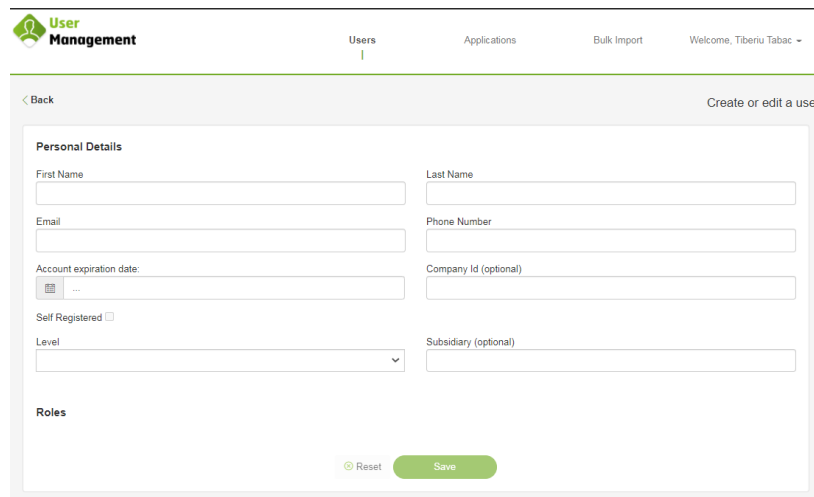
- i. accepted the Terms of use for end users of the ECB Identity Portal;
- ii. a mobile phone (for voice and text messages) or a desk phone (for voice messages) to receive the second part of the two-factor authentication.

To create a new user, an administrator logs in to the ECB Identity Portal, switches to User Management (iWelcome UI) and performs the following steps.

- a. Access the **Users** administration menu.
- b. Click **Create a new user** at the top-right corner of the panel (see the arrow below).

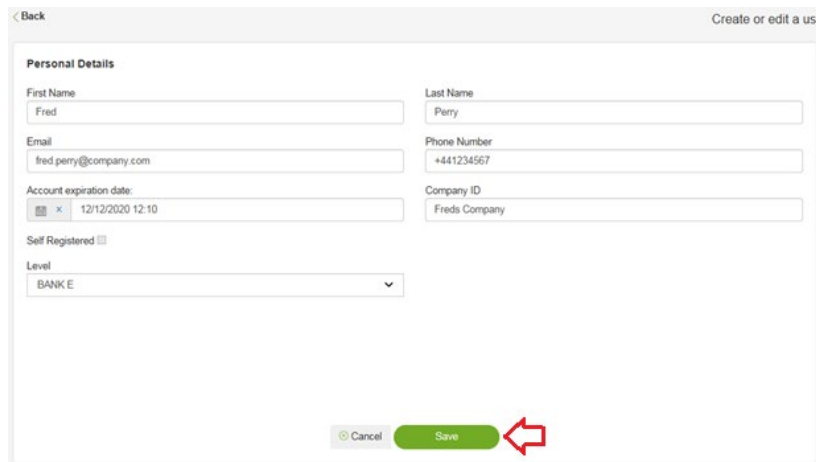


c. In the **Create or edit a user** panel, enter the user’s personal details as required:



- i. first name;
- ii. last name;
- iii. email address (linked to the user’s official organisation, e.g. a bank or academic institute, as per the terms and conditions);
- iv. phone number (including the country code, e.g. +49 for Germany or +353 for Ireland);
- v. expiration date (if the new account is temporary, set an expiration date);
- vi. company ID (only applies to certain applications);
- vii. level (the organisation to which the new user belongs).

Once complete, click **Save** to create the new user account.



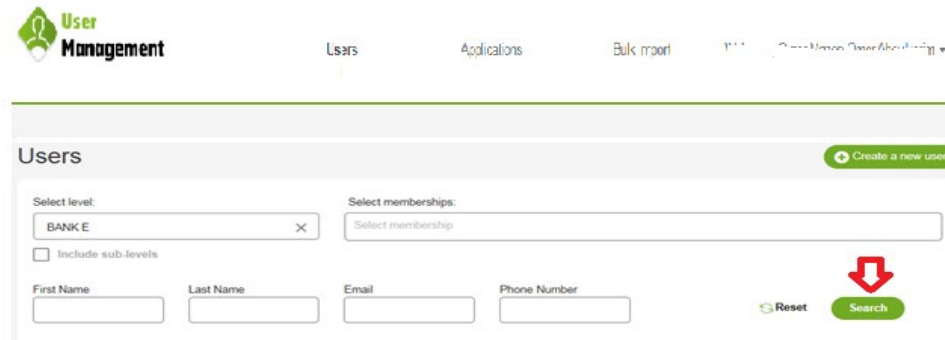
The new user account is created but will remain dormant until the user clicks the link in the activation email.

6.2. Editing a user’s details

The following procedure is only available to DUAs.

To edit or update user details, a DUA must perform the following steps.

- a. Access the [iWelcome UI](#) interface.
Go to the **Users** administration menu.



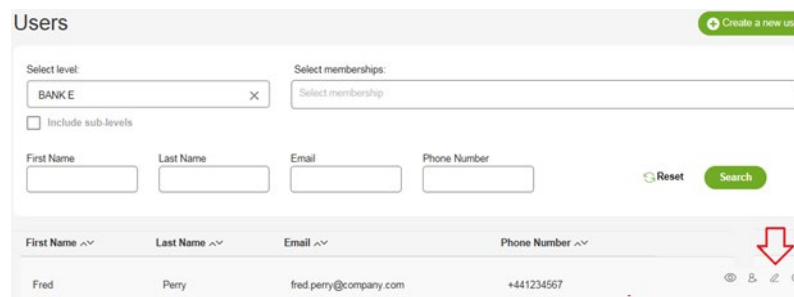
Set the available filters, where known:

- i. first name;
- ii. last name;
- iii. email address;
- iv. phone number.

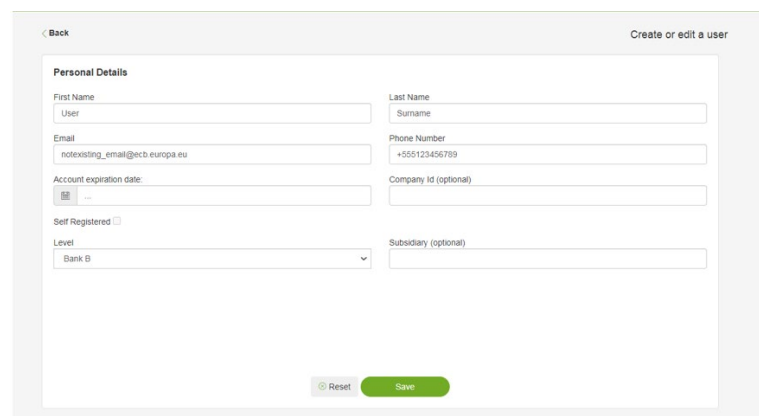
It is also possible to search by level (organisation) by selecting the level to which the user belongs.

Click **Search**.

Click the **Pencil icon** (see the arrow below) to edit the details for the specific user.



Modify or add more information to the fields that need changing or updating.

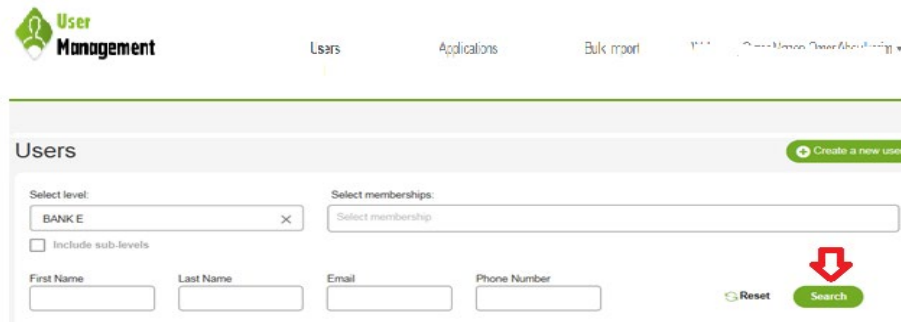


Click **Save**.

6.3. Suspending an account

DUAs can suspend the account of a DAA or general user. To suspend a user’s account, a DUA must perform the following steps.

- a. To search for a particular user, access the [iWelcome UI](#) interface. Go to the **Users** administration menu.



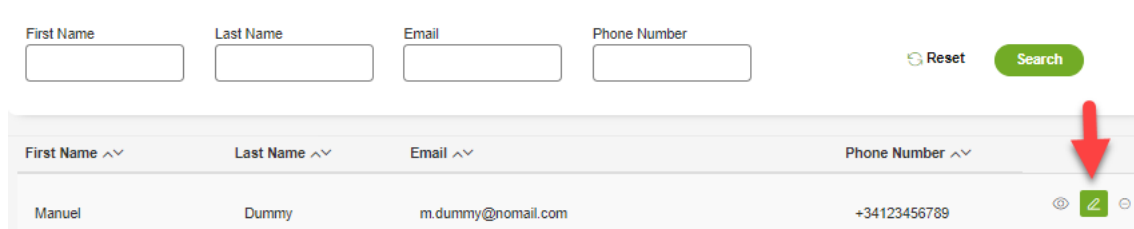
Set the available filters, where known:

- i. first name;
- ii. last name;
- iii. email address;
- iv. phone number.

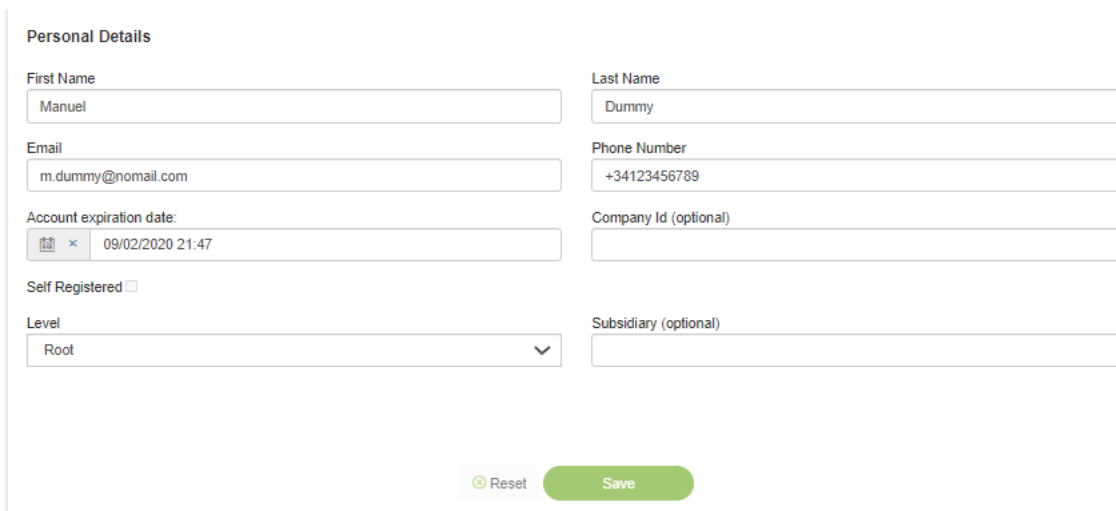
It is also possible to search by level (organisation) by selecting the level to which the user belongs.

Click **Search**.

Click the **Pencil icon** (see the arrow below) to edit the profile of the selected user account.



Change the account expiry date to the current date.



Click **Save**.

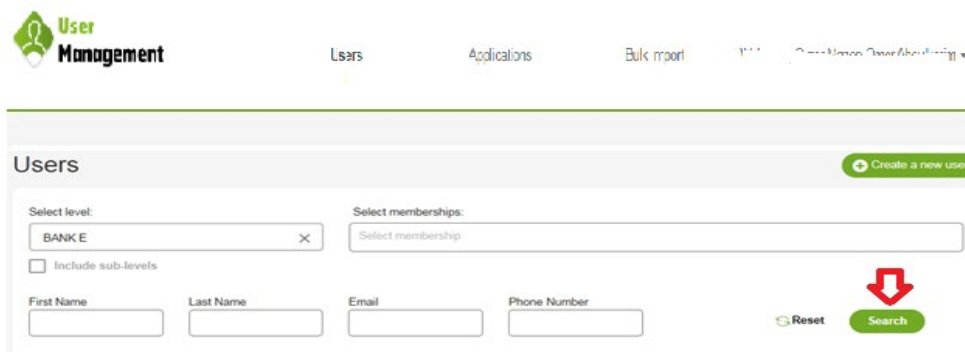
6.4. Deleting a user

There are three possible ways to delete a user account:

1. A DUA performs this task for members of their own organisation (see below).
2. A user does it using the [self-deletion](#) option on the **Security** page.
3. A user asks the ECB Support Centre to delete the account.

A DUA must perform the following steps to delete a user through the [iWelcome UI](#) interface.

- a. Go to the **Users** administration menu.



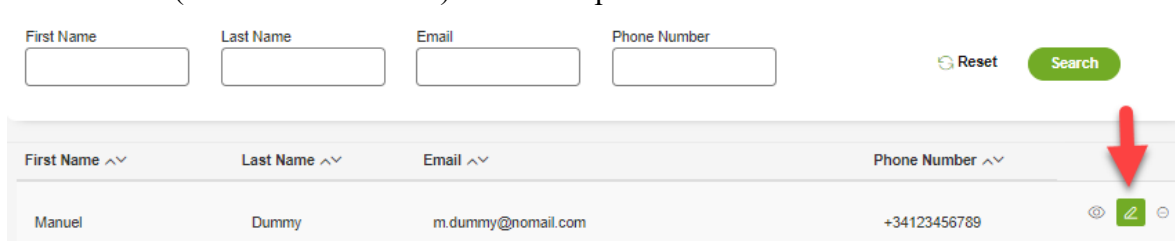
Set the available filters, where known:

- i. first name;
- ii. last name;
- iii. email address;
- iv. phone number.

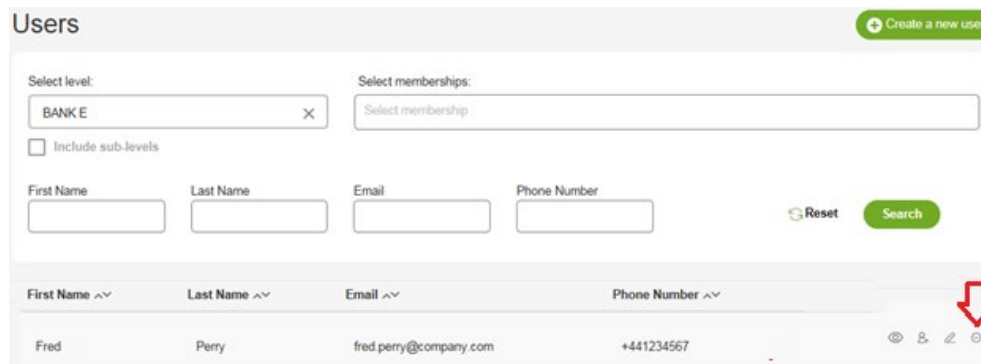
It is also possible to search by level (organisation) by selecting the level to which the user belongs.

Click **Search**.

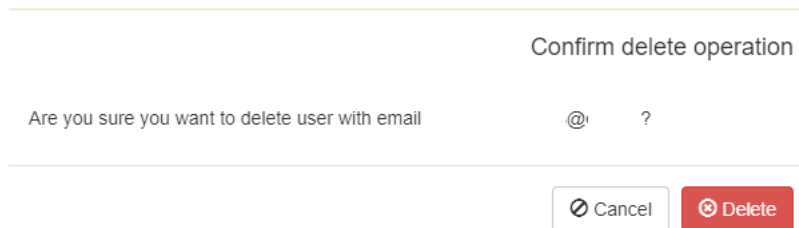
Click the **Pencil icon** (see the arrow below) to edit the profile of the selected user account.



Click the **(-) icon** to the right of the user’s name and contact details to delete (see the arrow below).



A pop-up will appear asking the DUA to confirm the delete operation.



Clicking **Delete** will remove the user.

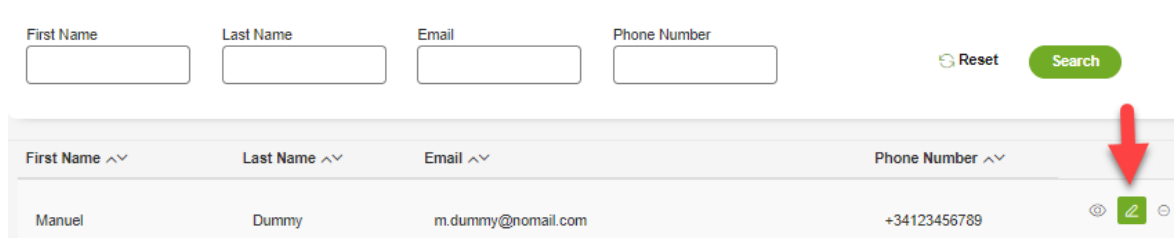
6.5. Granting a DUA role

A DUA can grant a DUA role within their own organisation.

To grant a DUA role, the DUA must perform the following steps.

- a. Log in through the [iWelcome UI](#) interface and go to the **Users** administration menu to edit a user.
- b. Select the level (organisation) of the user.
- c. Search for the user by using the available filters (see Section 6.3):
 - i. first name;
 - ii. last name;
 - iii. email address;
 - iv. phone number.

When the selected user is displayed, click the **Pencil icon** (see the arrow below).



Tick the “DelegatedUserAdmin” checkbox.

The screenshot shows a user profile form with the following fields:

- Personal Details:**
 - First Name: Manuel
 - Last Name: Dummy
 - Email: m.dummy@nomail.com
 - Phone Number: +35 00
 - Account expiration date: ...
 - Company Id (optional):
 - Self Registered:
 - Level: (dropdown menu)
 - Subsidiary (optional):
- Roles:**
 - DelegatedUserAdmin

Buttons: Reset, Save

Click **Save** to finish the operation.

6.6. Revoking a DUA role

A DUA can revoke a DUA role within their organisation.


To revoke a DUA role, the DUA must perform the following steps.

- a. Log in through the [iWelcome UI](#) interface and go to the **Users** administration menu to edit a user.
- b. Select the level (organisation) of the user.
- c. Search for the user by using the available filters (see Section 6.3):
 - i. first name;
 - ii. last name;
 - iii. email address;
 - iv. phone number.

When the selected user is displayed, click the **Pencil icon** (see the arrow below).

The screenshot shows a search interface with the following elements:

- Search filters: First Name, Last Name, Email, Phone Number.
- Buttons: Reset, Search.
- Table of results:

First Name ^v	Last Name ^v	Email ^v	Phone Number ^v	
Manuel	Dummy	m.dummy@nomail.com	+34123456789	

A red arrow points to the pencil icon in the table row.

Untick the “DelegatedUserAdmin” checkbox.

The screenshot shows a user profile form with the following sections:

- Personal Details:**
 - First Name: Manuel
 - Last Name: Dummy
 - Email: m.dummy@nomail.com
 - Phone Number: +35 30
 - Account expiration date: ...
 - Company Id (optional):
 - Self Registered:
 - Level: (dropdown menu)
 - Subsidiary (optional):
- Roles:**
 - DelegatedUserAdmin (highlighted with a red box)

At the bottom of the form, there are two buttons: "Reset" and "Save".

Click **Save** to finish the operation.

7. Delegated Access Administrator – specific tasks

Access to ECB portals is managed through user group memberships in the ECB Identity Portal. To access a specific ECB portal, a user needs to be assigned to at least one group granting access to that portal.

7.1. Confirming user group memberships

To review a user’s group memberships, a DAA must perform the following steps.

- a. Log in through the [iWelcome UI](#) interface and go to the **Users** administration menu to view, create, or edit a user’s group membership.

The screenshot shows the "Users" administration interface with the following elements:

- Buttons:** "Create a new user" (green)
- Select level:** Root (dropdown menu)
- Select memberships:** Select membership (dropdown menu)
- Include sub-levels:**
- Search filters:** First Name, Last Name, Email, Phone Number (input fields)
- Buttons:** "Reset" and "Search" (green)

Search for the user using the available filters:

- i. first name;
- ii. last name;

- iii. email address;
- iv. phone number;
- v. memberships.

View the user’s details by clicking the **Eye icon** (see the arrow below).

First Name	Last Name	Email	Phone Number	
Fred	Perry	fred.perry@company.com	+441234567	

The list of memberships is shown on the next panel (highlighted in yellow below).

Field	Value
ID	029c97b6-bc73-45ba-b95e-bb5ed4a72036
First Name	Fred
Last Name	Perry
Email	fred.perry@company.com
Phone Number	+441234567
Company ID	Freds Company
Self Registered	None
Groups	<ul style="list-style-type: none">BankE_App3_Grpbank_e_app_group
Manager Groups	<ul style="list-style-type: none">UserAdmin
Assignable Applications	None
Account expiration date:	12/12/2020, 12:10:00
Level	BANK E
Preferred language:	en_GB
Created:	12/02/2020, 13:32:37
Last modified:	12/02/2020, 14:35:39

7.2. Adding a user to a user group (membership)

To assign a group membership to a user, a DAA must perform the following steps

- a. Log in through the [iWelcome UI](#) interface, go to the **Users** administration menu to edit a user.

The screenshot shows the 'Users' management interface. At the top right is a '+ Create a new user' button. Below it are two dropdown menus: 'Select level:' with 'Root' selected and 'Select memberships:' with 'Select membership' selected. There is an 'Include sub-levels' checkbox. Below these are four input fields labeled 'First Name', 'Last Name', 'Email', and 'Phone Number'. To the right of these fields are 'Reset' and 'Search' buttons.

Search for the user using the available filters:

- i. first name;
- ii. last name;
- iii. email address;
- iv. phone number.

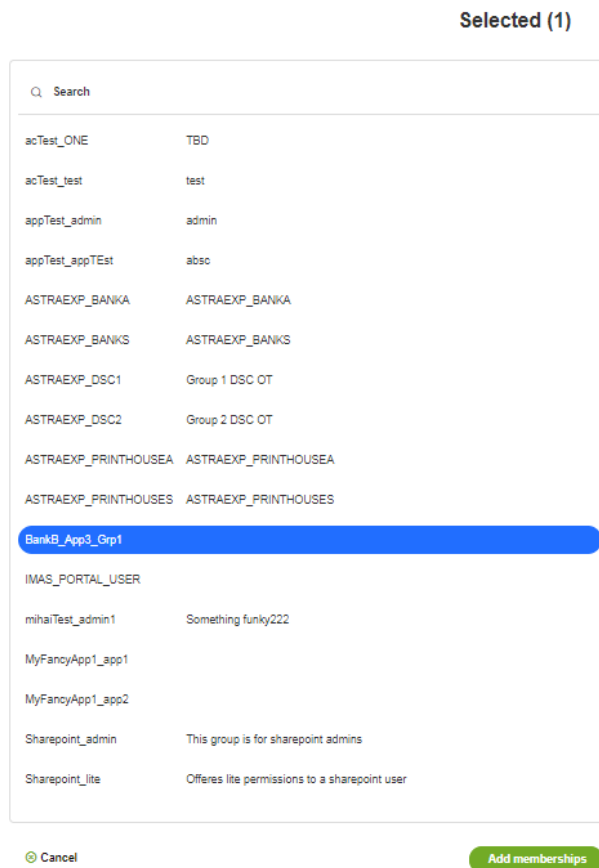
Once the user is found, click the **Assign Memberships icon** (see the arrow below).

This screenshot shows the search results in the 'Users' interface. The search filters are 'Select level: BANK E' and 'Include sub-levels' is unchecked. The search results table has columns for 'First Name', 'Last Name', 'Email', and 'Phone Number'. One user is listed: Fred Perry, fred.perry@company.com, +441234567. To the right of the user's name is an action menu with icons for view, edit, and assign memberships. A red arrow points to the assign memberships icon.

On the **Assign Memberships** panel, search for the membership that is to be assigned to the user.

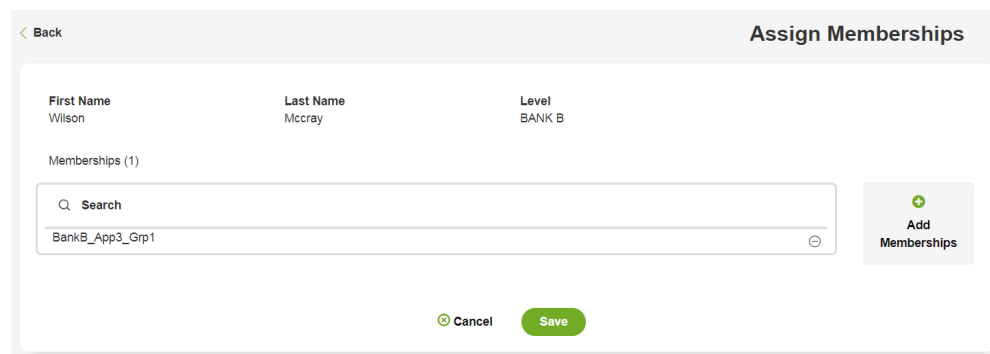
The screenshot shows the 'Assign Memberships' panel. At the top left is a '< Back' button. The user's details are displayed: 'First Name: Wilson', 'Last Name: Mccray', and 'Level: BANK B'. Below this is a section for 'Memberships (0)' with a search bar. To the right is a '+ Add Memberships' button. At the bottom are 'Cancel' and 'Save' buttons.

Select the required membership (highlighted in blue below).



Once selected, click **Add memberships**.

Click **Save** to finish assigning memberships to the user.



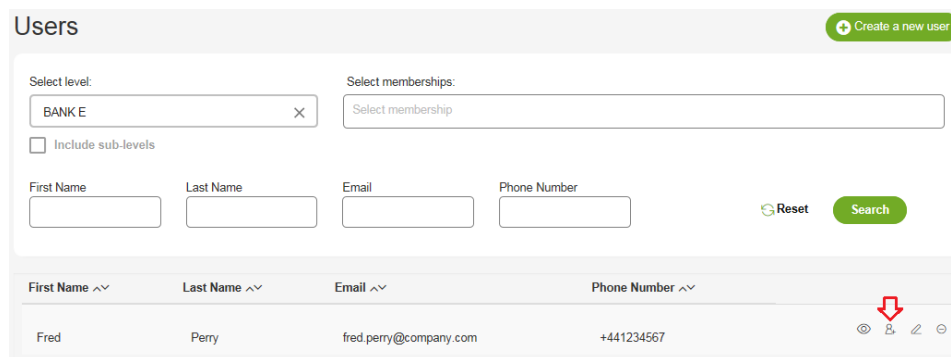
To confirm the groups/memberships to which a user is subscribed, search for the user and view their details following the steps set out in [Section 7.1 – Confirming user group memberships](#).

7.3. Deleting a user from a group

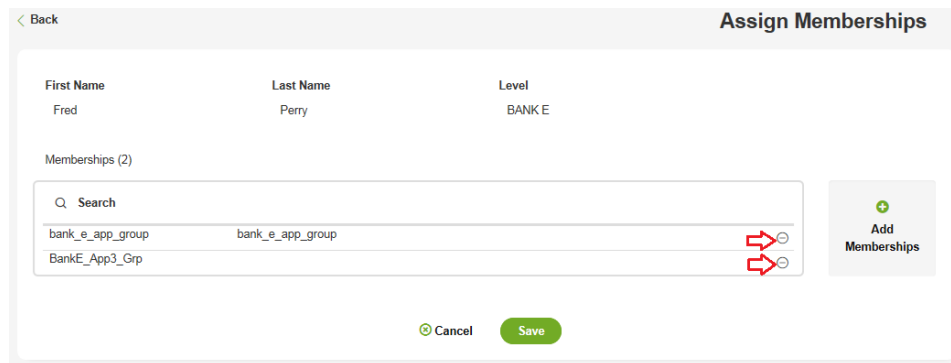
Deleting a user from a group is similar to the process for adding a user to a group. To delete a user from a group, a DAA must perform the following steps.

- a. Log in through the [iWelcome UI](#) interface and go to the **Users** administration menu to delete a user from a group.
- b. Select the level (organisation) of the user.
- c. Search for the user by using the available filters (see Section 6.3):
 - i. first name;
 - ii. last name;
 - iii. email address;
 - iv. phone number.

When the selected user is displayed, click the **Assign Memberships icon** (see the arrow below).



In the selected group, click the **(-) icon** on the right-hand side to delete.



Click **Save** to finish the operation.

7.4. Granting a DAA role

DAAs can only grant a DAA role for applications for which they are responsible.

To grant a DAA role, the DAA must perform the steps.

- a. Log in through the [iWelcome UI interface](#) and go to the **Users** administration menu to edit a user.
- b. Select the level (organisation) of the user.
- c. Search for the user by using the available filters (see Section 6.3):
 - i. first name;
 - ii. last name;
 - iii. email address;

iv. phone number.

When the selected user is displayed, click the **Pencil icon** (see the arrow below).

First Name	Last Name	Email	Phone Number	Reset	Search
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
First Name ^v	Last Name ^v	Email ^v	Phone Number ^v		
Manuel	Dummy	m.dummy@nomail.com	+34123456789		

Tick the “ApplicationAccessAdmin” checkbox.

< Back

Personal Details

First Name: Manuel
Last Name: Dummy
Email: m.dummy@nomail.com
Phone Number: +35 30
Account expiration date: ...
Company Id (optional):
Self Registered:
Level:
Subsidiary (optional):

Roles

ApplicationAccessAdmin

Applications: appTest | Add | Remove

Reset Save

Select the application(s) that will be managed by the new DAA and click **Add**, as indicated below.

< Back

Personal Details

First Name: Manuel
Last Name: Dummy
Email: m.dummy@nomail.com
Phone Number: +35 30
Account expiration date: ...
Company Id (optional):
Self Registered:
Level:
Subsidiary (optional):

Roles

ApplicationAccessAdmin

Applications: appTest | Add | Remove

Reset Save

Back

Personal Details

First Name: Manuel
Last Name: Dummy
Email: m.dummy@nomail.com
Phone Number: +35 00
Account expiration date: ...
Company Id (optional):
Self Registered:
Level:
Subsidiary (optional):

Roles

ApplicationAccessAdmin

Applications

→ Add appTest
← Remove

Reset Save

Click **Save** to finish the operation.

7.5. Revoking a DAA role

DAAs can only revoke a DAA role for applications for which they are responsible.

To revoke a DAA role for a specific application, the DAA must perform the following steps.

- a. Log in through the [iWelcome UI interface](#) and go to the **Users** administration menu to edit a user.
- b. Select the level (organisation) of the user.
- c. Search for the user by using the available filters (see Section 6.3):
 - i. first name;
 - ii. last name;
 - iii. email address;
 - iv. phone number.

When the selected user is displayed, click the **Pencil icon** (see the arrow below).

First Name Last Name Email Phone Number

Reset Search

First Name ^v	Last Name ^v	Email ^v	Phone Number ^v	
Manuel	Dummy	m.dummy@nomail.com	+34123456789	

Select the application(s) for which the DAA is no longer responsible and click **Remove** as indicated below.

The image displays two sequential screenshots of a user management interface. The top screenshot shows the 'Personal Details' section with fields for First Name (Manuel), Last Name (Dummy), Email (m.dummy@nomail.com), Phone Number (+35 30), and Account expiration date. The 'Roles' section shows the 'ApplicationAccessAdmin' checkbox checked. Below this, the 'Applications' section has an 'Add' button highlighted with a red box, and a dropdown menu showing 'appTest'. The bottom screenshot shows the same interface, but the 'Remove' button is highlighted with a red box, and 'appTest' is now listed in the 'Applications' list. Both screenshots include 'Reset' and 'Save' buttons at the bottom.

Click **Save** to finish the operation.

Note that unticking the “ApplicationAccessAdmin” checkbox affects the management of **all applications** for which the DAA is responsible, and the role is also revoked for those applications not visible to the current DAA.

< Back

Personal Details

First Name Manuel	Last Name Dummy
Email m.dummy@nomail.com	Phone Number +35 30
Account expiration date: ...	Company Id (optional)
Self Registered <input type="checkbox"/>	Subsidiary (optional)
Level ▼	

Roles

- ApplicationAccessAdmin

Reset Save

Annex 1 – FAQs and automated responses

Frequently Asked Questions

The FAQs can be found below the Log in button on the **ECB applications** login page.

EUROPEAN CENTRAL BANK | EUROSYSTEM
ECB Identity Portal

Log in to ECB applications

Email Address *

Password *

Log in

[Activate or reset password](#) [Frequently Asked Questions](#)

[Login from ECB network | Privacy statement](#)

The current FAQs, together with the answers, are shown below.

How do I gain access to an ECB application?

If you already have a login account, please contact the relevant Delegated Access Administrator in your organisation or your ECB counterpart for advice on how to gain access to an ECB application.

Otherwise, please see “How can I get an account and/or update my personal details?”.

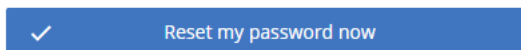
How can I get an account and/or update my personal details?

If you require an account or need to change other details such as your email address, please get in touch with your relevant contact person. If your account is managed by a local department within your organisation, you will need to contact your Delegated User Administrator. If your account is managed by the ECB, please contact your ECB counterpart.

If you already have an account, you can update your telephone number, change your password or delete your account by logging in to your profile page.

How can I activate, reset or change my account password?

To obtain a link to activate your account or to change/reset your password, please click the **Reset my password now** link, as shown below.



What are my login options?

You can log in with a password and a second authentication factor, which is obtained by text or voice message.

The **Login from ECB network** option is only for users who are connected to the ECB network and have an @ecb.europa.eu email address.

I am having issues with my account. Who can I contact for help?

Please contact the ECB Support Centre by email at supportcentre@ecb.europa.eu or by phone on +49 69 1344 7766.

Automated processes – screenshots

The following emails are generated automatically in response to a user’s actions.

<p>Account registration</p>	<p>Password is about to expire</p>	<p>Password reset</p>
------------------------------------	---	------------------------------