EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB Identity Portal User Manual

General and IMAS portal-specific
04 March 2024

TABLE OF CONTENTS

DEFINITION AND GLOSSARY

The European Central Bank (ECB) Identity Portal (https://id.ecb.europa.eu) is the online platform for the central identification, authentication and account management of users of ECB applications that are accessible to third parties.

User accounts can be managed by:

- ECB staff
- A third party through Delegated User Administrators and Delegated Access Administrators nominated by the third-party and confirmed by ECB staff

For assistance, please contact the ECB Support Centre at supportcenter@ecb.europa.eu or +49 69 1344 7766.

Glossary:

User: an authenticated and authorised natural person, who, on behalf of a third party, has access to the ECB Identity Portal and is assigned access rights in accordance with their role.

Delegated User Administrator (DUA): an authenticated and authorised natural person, who, on behalf of a third party, can manage users of their organisation that might have access to ECB managed applications.

Delegated Access Administrator (DAA): an authenticated and authorised natural person, who, on behalf of a third party, can assign application access rights to third-party users created by the DUA, in accordance with their role.

Third party: a legal person that interacts with the European Central Bank (ECB).

The roles and responsibilities of users are detailed in the "Terms of use for end users of ECB Identity Portal" and "Terms of use – supplement for Delegated User and Access Administrators (DUAs and DAAs) of ECB Identity Portal".

PROCEDURES

1. LOGIN

Logging into the ECB Identity Portal requires two-factor authentication.

The login window below (Fig.1) is shown when the user accesses, via a browser, the ECB Identity Portal at https://id.ecb.europa.eu.

Login step one: Provide user email and password.

Login step two: Provide the six-digit code sent to the user's mobile number via SMS or voice message.

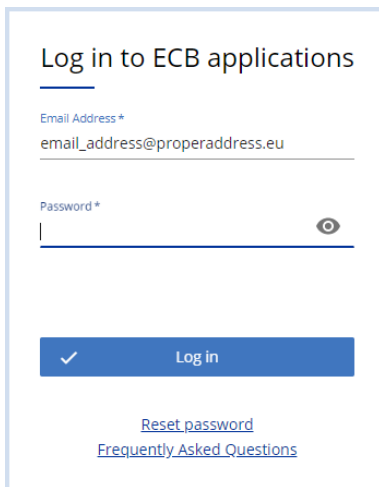(NB: The code expires after three minutes and the procedure has to be restarted.)
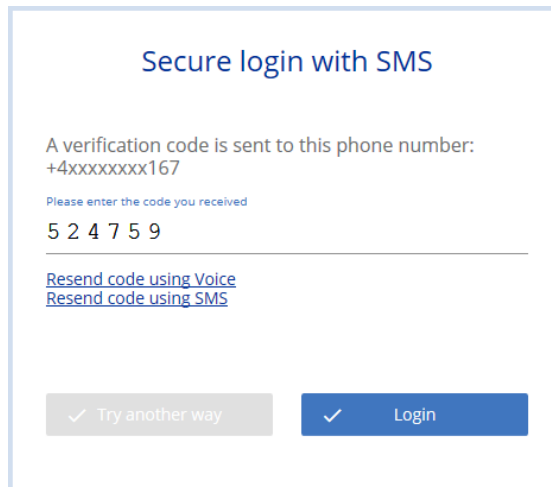
Fig.1, Login Step one   Fig.2, Login Step two

The user can change the authentication method by selecting either "Resend code using Voice" or "Resend code using SMS" (Fig.2). This will restart the login process. The method chosen will become the default.

2. USER PROFILE AND MY APP PAGE

On the "Security" tab of the user's profile page there is an option to change the user's password and phone number.
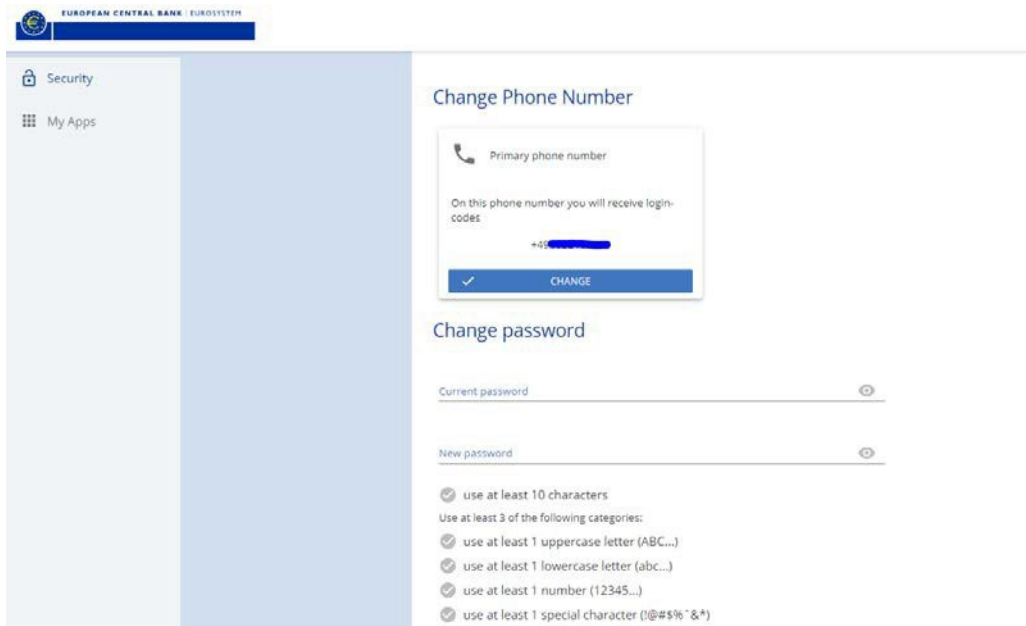
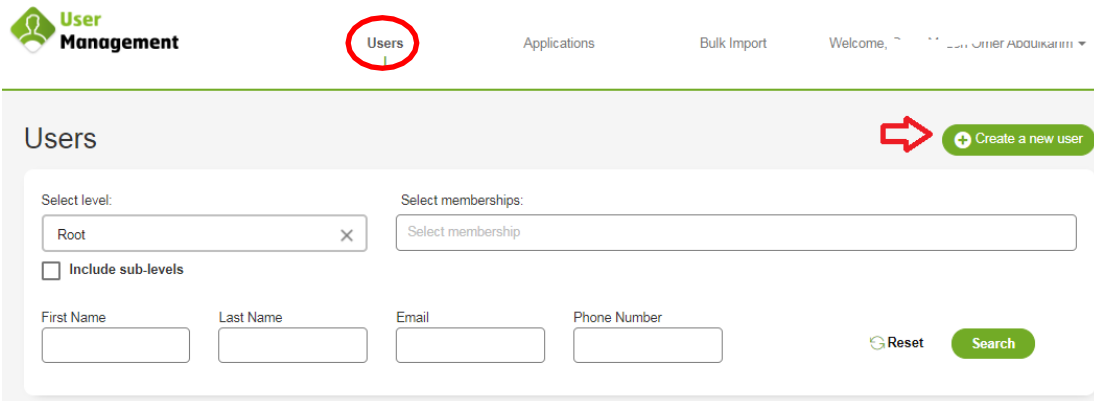The "My Apps" tab lists the authorised applications.
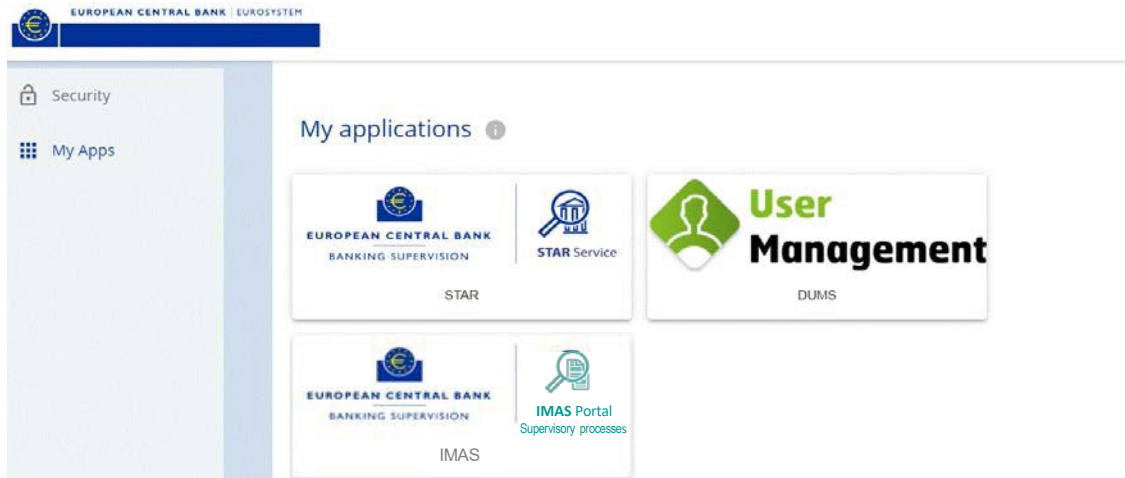
3. CREATE, DELETE AND MODIFY USERS

Only "Delegated User Administrator" can create, delete and modify user accounts.
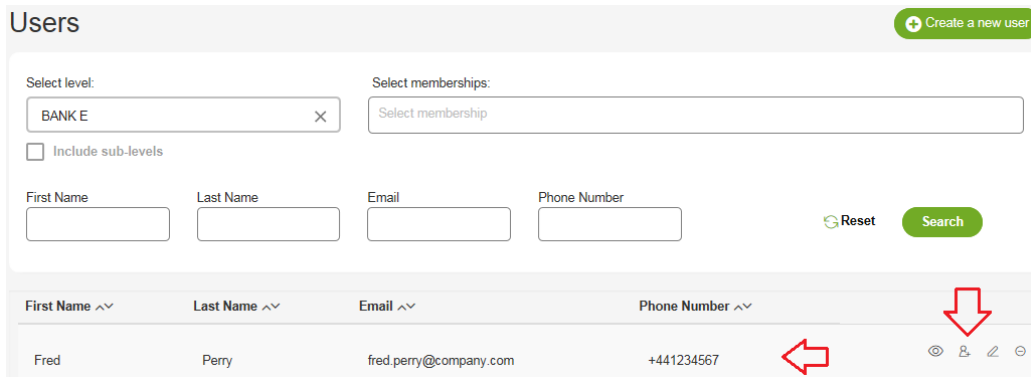
To create a new user, an administrator must:

  a. Access the "**Users**" administration menu;
  b. Click on "**Create a new user**" in top right corner;

  c. Enter the following information:
      i. First Name
     ii. Last Name
    iii. Email
     iv. Phone Number (use international format e.g. for Germany +49, etc.)
      v. Company ID – this field is optional, only applicable to specific applications
     vi. Account Expiration Date – (for temporary accounts)
  d. Save the information.

The following actions can be performed for each individual user, using icons indicated in the image below: view, assign membership, edit and delete.
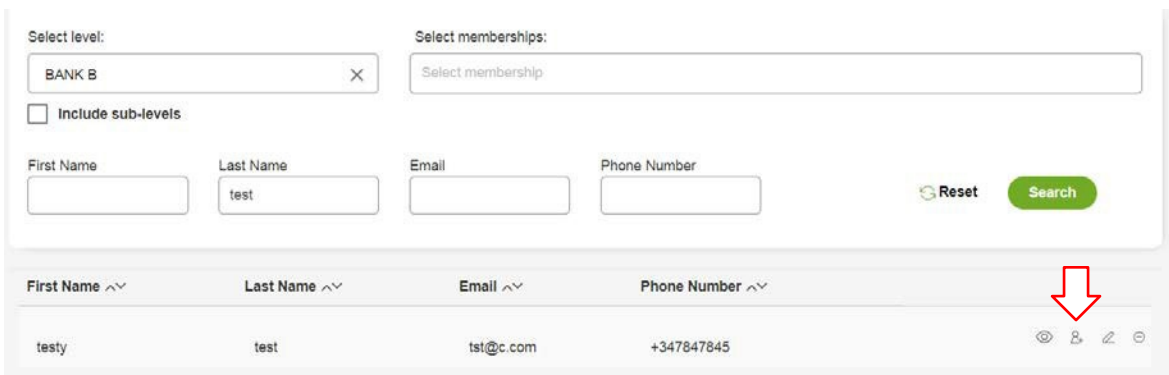
4. PROVIDE ACCESS TO ECB APPLICATIONS

Only a "**Delegated Access Administrator"** can provide access to ECB applications.

User access must be enabled for ECB applications (e.g. ASTRA, IMAS, etc.) by an administrator assigning a group membership.

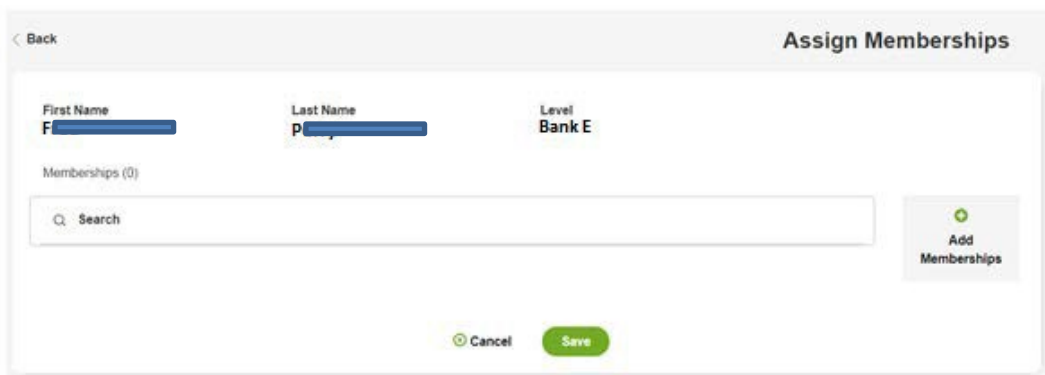Group membership is assigned through using the "**Assign membership**" button as illustrated below:
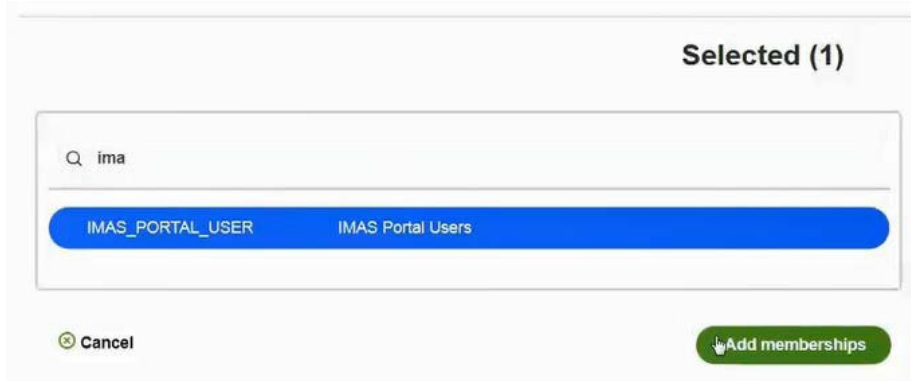
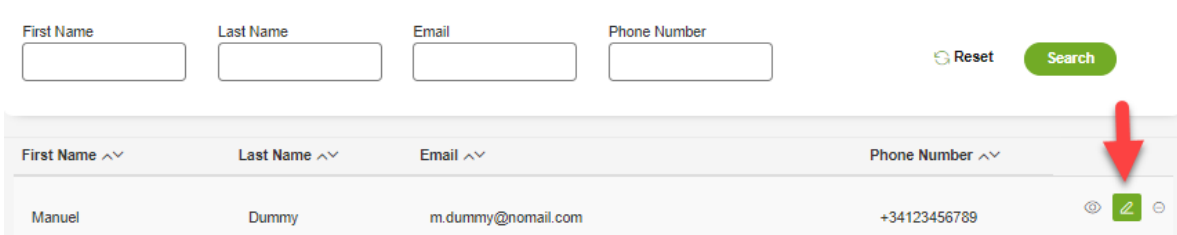Click "**Save**" to finish the assigning group membership.

Group membership will grant predefined permission levels for the selected application. For some applications (e.g., the IMAS portal), administrators may set more specific permissions using the **user management system** in the relevant application (see the section 6).

Access to the applications can be removed using the same interface.

5. GRANT DELEGATED ADMINISTRATOR ROLES

Only users with a "Delegated Access Administrator" (DAA) role can grant DAA privileges to other users. The same applies to "Delegated User Administrators" (DUAs).

Administrator roles are granted and revoked by **editing an existing user**:
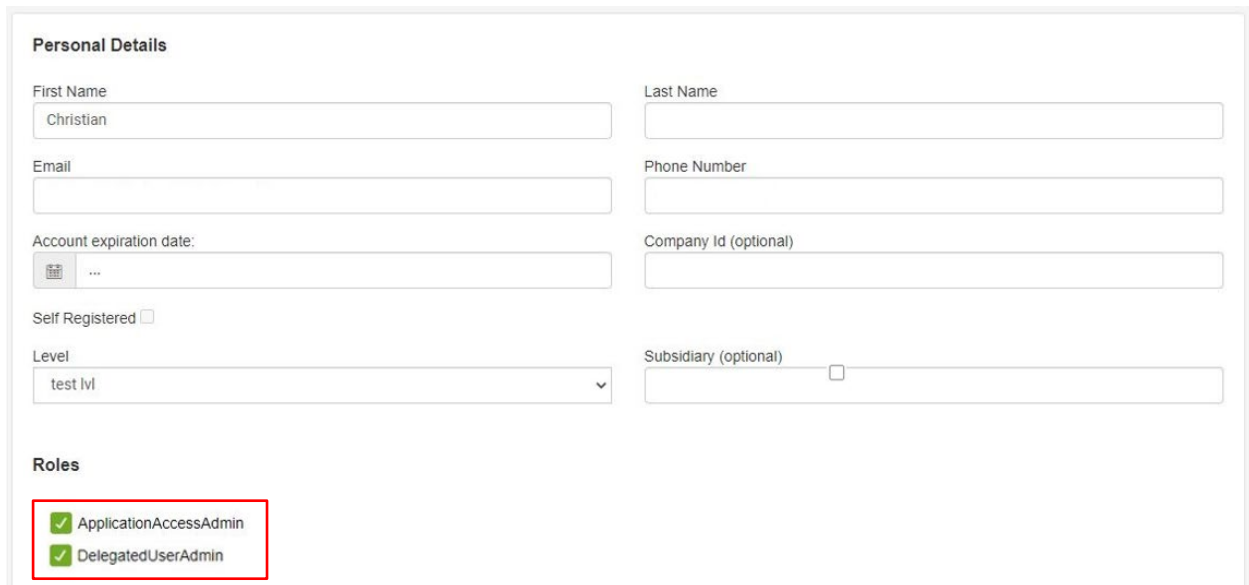

If you are a Delegated Administrator, you will see the **Roles** section below the user's **Personal Details**.

In this section:
▪ DAAs will be able to grant and revoke the **ApplicationAccessAdmin** role only for the application(s) they manage. Unless they are also DUAs, they will not be able to modify the user's account details.
▪ DUAs will be able to grant and revoke the **DelegatedUserAdmin** role.

To remove Administrator privileges, simply untick the relevant checkbox.

Save your changes.

6. MANAGING USER PERMISSIONS IN THE IMAS PORTAL

Only users with a "Delegated Access Administrator" (DAA) role can manage user permissions in the IMAS portal. When a new user logs into the IMAS portal for the first time, an account is automatically created.

To manage user permissions in the IMAS portal an administrator must take the following steps.

Select the "**Manage Users**" tab on the dashboard page, or type in this URL: https://imas.ecb.europa.eu/useradmin/

1. Click on the Manage Users tab
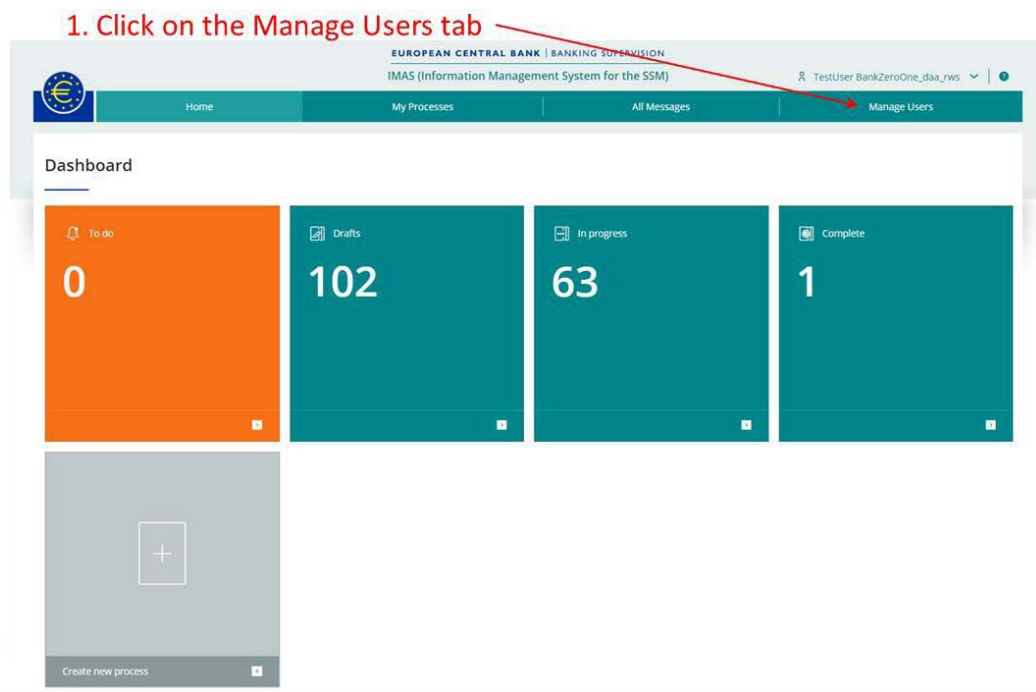
If the new user is not displayed after first logon, the DAA should refresh the "Manage Users" page. When the user whose permissions need to be modified is visible in the listing, the DAA selects the user and makes the necessary modifications.

After the DAA has granted the necessary permissions to the new user, the user should refresh the IMAS portal page to see the effect of the newly granted permissions.