ECHA
EUROPEAN CHEMICALS AGENCY

For the nominated User Administrators at national authorities

Identity and Access Management (IAM) Portal User Manual

Version 1.3

Version	Changes	Date
1.0	First version	February 2016
1.1	IUCLID6 permissions Service requests management updates	June 2016
1.2	Business roles description updated	September 2016
1.3	Business role update (PCN Normal), minor editorial changes	April 2019

Identity and Access Management (IAM) Portal User Manual

ECHA reference number: ECHA-16-B-05-EN
Publ.date: April 2019

Language: EN

If you have questions or comments in relation to this document please send them (quote the reference and issue date) using the information request form. The information request form can be accessed via the Contact ECHA page at: http://echa.europa.eu/about/contact_en.asp

European Chemicals Agency

Mailing address: P.O. Box 400, FI-00121 Helsinki, Finland
Visiting address: Annankatu 10, Helsinki, Finland

Table of Contents

Table of Figures

1. Introduction

1.1 Scope and pre-conditions

This document details the Identity and Access Management (IAM) functionalities for User Administrators.

ECHA provides a dedicated secure access to ECHA's Information systems for the Member State Competent Authorities (MSCAs)/ Mandated National Institutions (MNIs)/ Designated National Authorities (DNAs), the European Commission (COM) and Appointed Bodies. The remote access architecture is based on SSL VPN[1] model.

In order to establish a secure connection to IAM, the User Administrator needs:

- RSA token and the credentials (username/one-time-password) provided by ECHA
- Internet connection

1.2 What can I do in IAM Portal?

The IAM Portal is a centralized hub with self-service capabilities for access and service management requests. It helps the nominated User Administrators to autonomously manage access rights through business roles for all users under their responsibility.

Making use of IAM Portal, User Administrators can manage all different types of requests (create/suspend accounts, join/leave business roles, service requests, etc.) without requiring help from ECHA.

IAM Portal is based on a RBAC model (role based access control), hence it reduces the complexity in requesting detailed and fine-grained application permissions. It improves the response and resolution time for all access requests. Users are able to request access based on their role in the national authorities, rather than on-off user access rights requests. Moreover, the User Administators can grant access to multiple systems simultaneously based on predefined business roles tailored to the job responsibilities of their organisation.

[1] An SSL VPN is a form of VPN that can be used with a standard Web browser.

2. ECHA Remote Access Portal

⚠	If this is the first time you are accessing ECHA Remote Access Portal, check first section 2.2 First time logon to ECHA Remote Access Portal

2.1 Login to the IAM Portal

Access ECHA Remote Access Portal via https://echa-access.echa.europa.eu

- In the field 'Username', type your userID
- In the field 'Passcode' type your PIN followed by Tokencode in your RSA token and click 'Sign In'

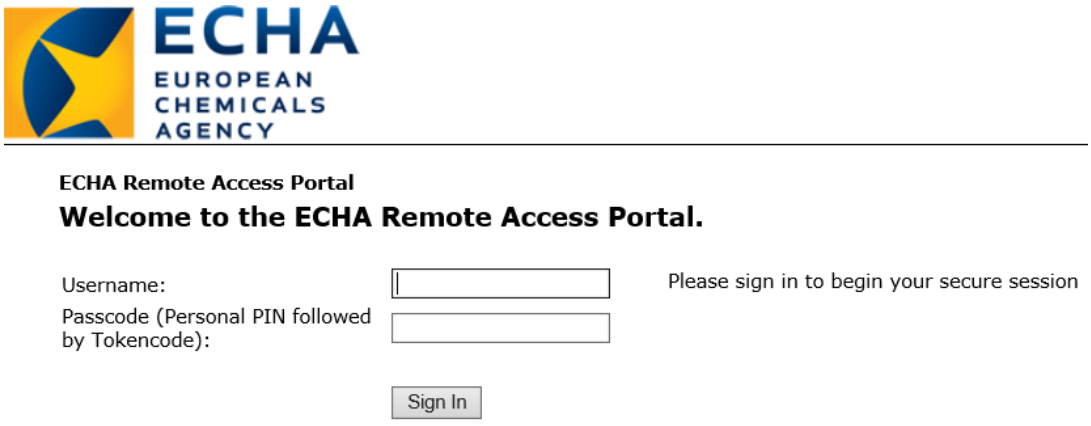

Figure 1: ECHA Remote Access Portal Login page

On ECHA Remote Access Portal, you can see the web-Bookmarks available for User Administrators (Figure 2: ECHA Remote Access Portal Login page – Web Bookmarks).

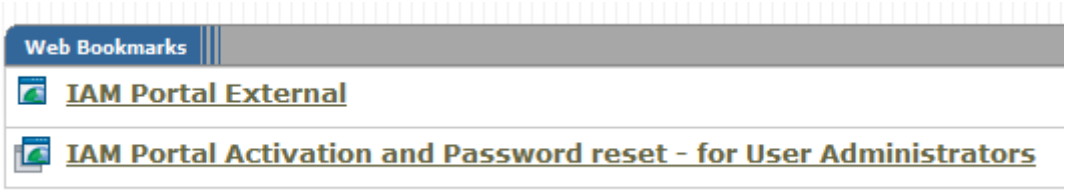

Figure 2: ECHA Remote Access Portal Login page – Web Bookmarks

2.2 First time login to ECHA Remote Access Portal

If this is the first time you are accessing ECHA Remote Access Portal, then you need to activate your token and set your PIN code.

- Access the ECHA Remote Access Portal via https://echa-access.echa.europa.eu
- In the field 'Username', type your userID
- In the field 'Passcode' type the 6-digit Tokencode (Figure 3: Tokencode) you see on your token screen

Figure 3: Tokencode

- Set up a Personal Identification Number (PIN) for your token, it should be 4 to 8 characters long. Make sure you remember your PIN without needing to keep a written record for it.

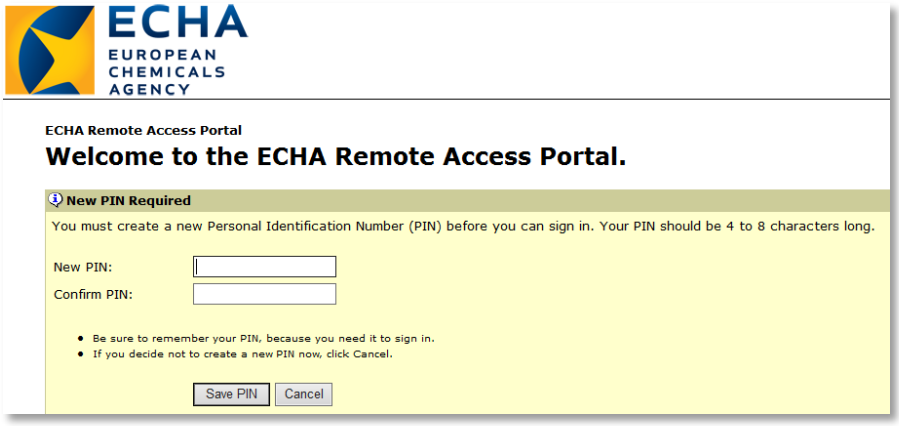

Figure 4: Setting a new Personal Identification Number (PIN)

- Once you save your PIN, you will be logged out automatically and taken back to the homepage.

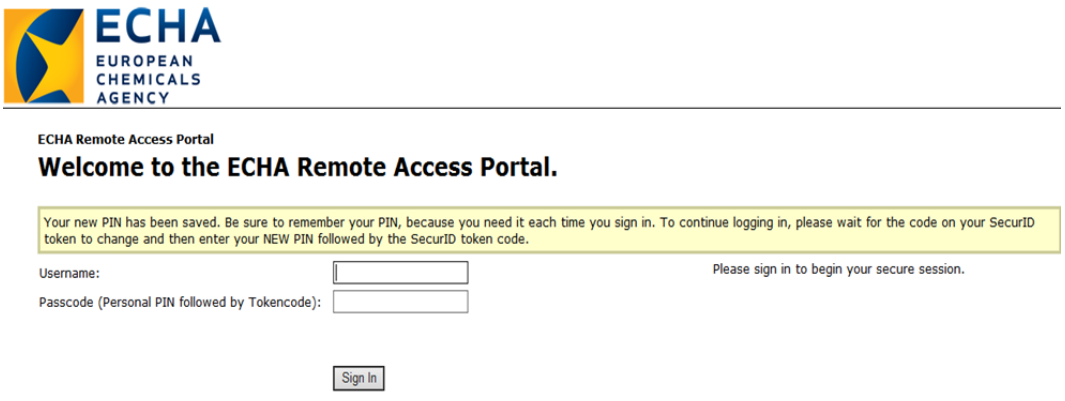

Figure 5: ECHA Remote Access Portal Login page – PIN set successfully

3. IAM Portal

3.1 Login to the IAM Portal

Click on 'IAM Portal External' bookmark (Figure 2: ECHA Remote Access Portal Login page – Web Bookmarks.

- In the field 'Username', type your userID
- In the field 'Password' type your current password
- In the field 'Domain', type 'External'

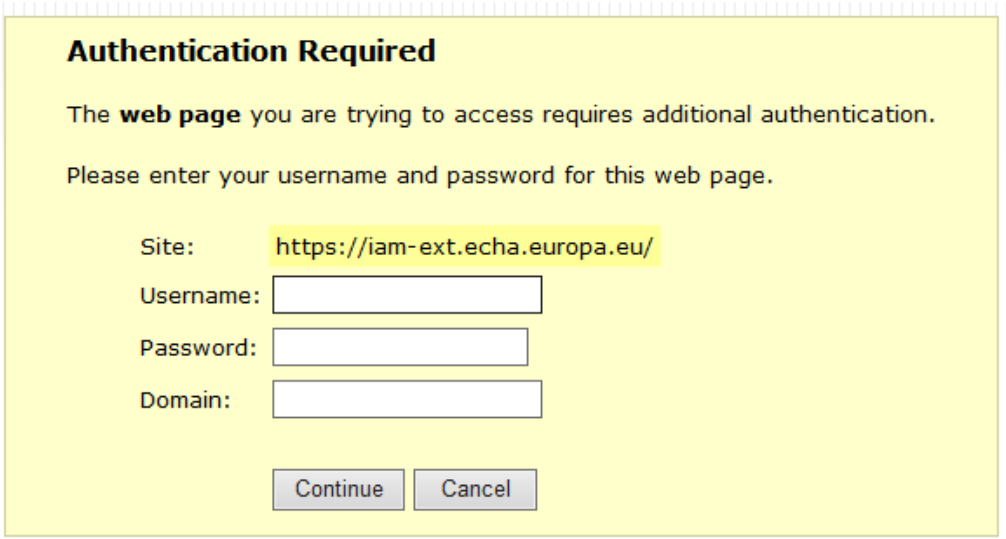

Figure 6: ECHA Remote Access Portal Login page – Bookmarks: IAM Portal

After loging-in successfully into the IAM Portal, you will be able to see the welcome screen of the portal (Figure 7: Welcome screen in the IAM portal).

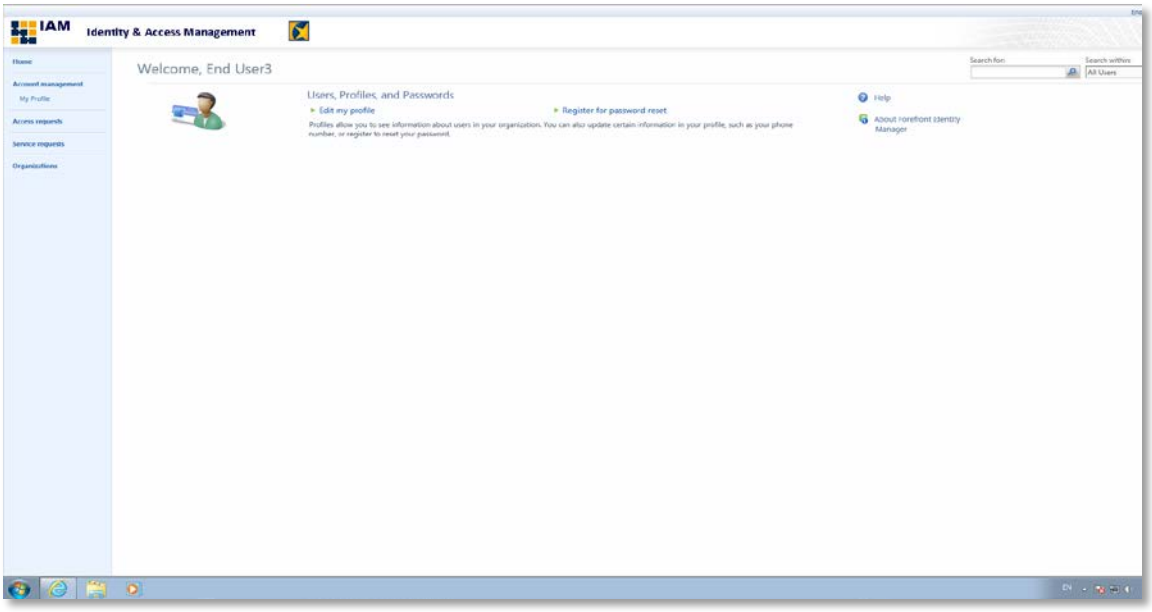

Figure 7: Welcome screen in the IAM portal

3.2 First time Login to IAM Portal

If it is the first time you are accessing IAM Portal, then you need to first activate your account.

- click on the link "IAM Portal Activation and Password reset - for User Administrators". Then you will be redirected to the following page (Figure 8: IAM Portal Activation and Password reset Login page); type your username (mXXZZZ or eXXZZZ) followed by the one-time password (OTP) ECHA provided you with.

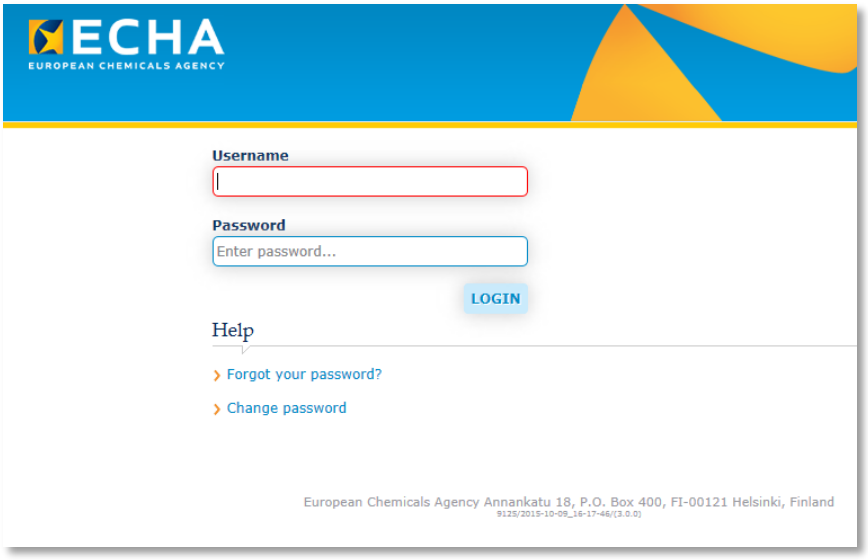

Figure 8: IAM Portal Activation and Password reset Login page

- When prompted, click 'here' to change the temporary password to your own (Figure 9: IAM Portal Activation – changing OTP step 1)

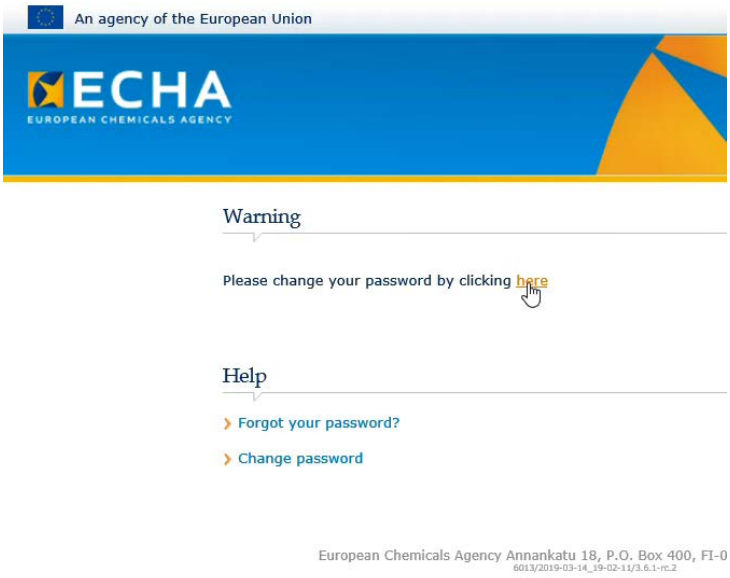

Figure 9: IAM Portal Activation – changing OTP step 1

- Type your username and your temporary password and click on 'Submit'

Figure 10: IAM Portal Activation – changing OTP step 2

- Provide your own password (Figure 11: IAM Portal Activation – changing OTP step 3)

Figure 11: IAM Portal Activation – changing OTP step 3

- A confirmation message appears. At this stage, click on the S button (Figure 12: IAM Portal Activation – changing OTP step 4).
  You will be re-directed to the home page; you can now login by clicking the link 'IAM Portal External'

Figure 12: IAM Portal Activation – changing OTP step 4

3.3 IAM password reset and change functionality

You can also reset your IAM Portal password or change it any time by selecting the "IAM Portal Activation and Password reset - for User Administrators" (Figure 2: ECHA Remote Access Portal Login page – Web Bookmarks).

Select option 'Forgot your password' if you want to reset your password (Figure 13: IAM Portal Activation and Password reset – Reset and change functionalities). If you want to change your password, select 'Change password'. Remember that you can reset your password as many times as you want during a day, however you can change your password only once a day.

Figure 13: IAM Portal Activation and Password reset – Reset and change functionalities

⚠	If you are a User Administrator but also have access with the same account to other IT tools (e.g.R4BP 3, REACH-IT, IUCLID, ePIC, Interact Portal) as 'normal End-user', note that **resetting or changing your password at this stage (for IAM Portal), also resets your password for the other IT tools as well**. This is because all those IT tools share a common authentication mechanism.

4. Account Management

4.1 Creating a new user account

To create a new user account for your Organization, you need to select **Account Management** from the left-hand side and then click on 'New'.

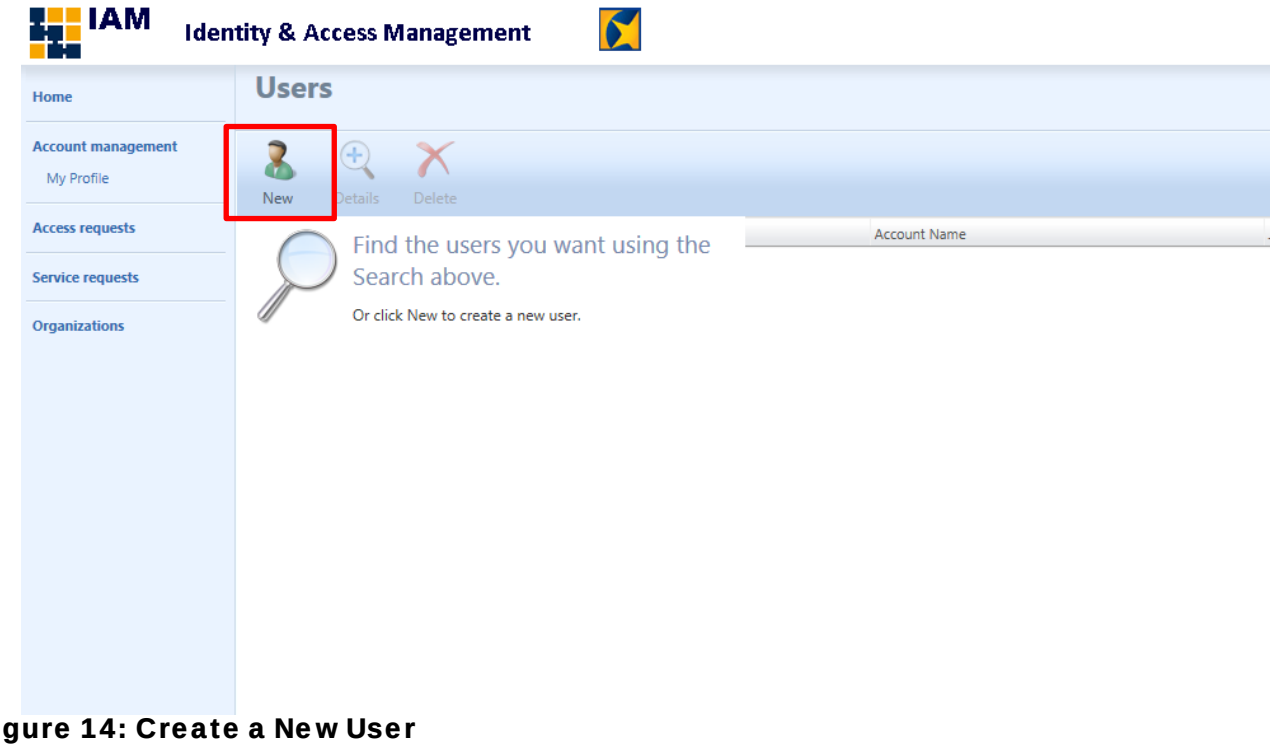

Figure 14: Create a New User

The **Create User** page (Figure 15: User creation page) opens. Fill in all mandatory fields (*) for the new user.
Users' names can contain various characters but must in IAM Portal be restricted to latin characters A-Z and underscores(_). Apostrophes, hyphens, spaces and similar must be omitted, and should be replaced by an underscore. Diacritical marks on latin letters A-Z are simply omitted and the following transliterations are permitted: Å→AA, Ä→AE, Ñ→NXX, Ö→OE, Ø→OE, Ü→UE or UXX. Other transliterations are Þ→TH, Æ→AE, Œ→OE and ß→SS.
'Organization' field: IAM portal allows you to type the Organization and then validate it by clicking the green check symbol.

⚠	If you need a new token for your user, leave the field 'RSA Token'blank. If you want to re-assign an existing token, please fill-in the token's serial number.

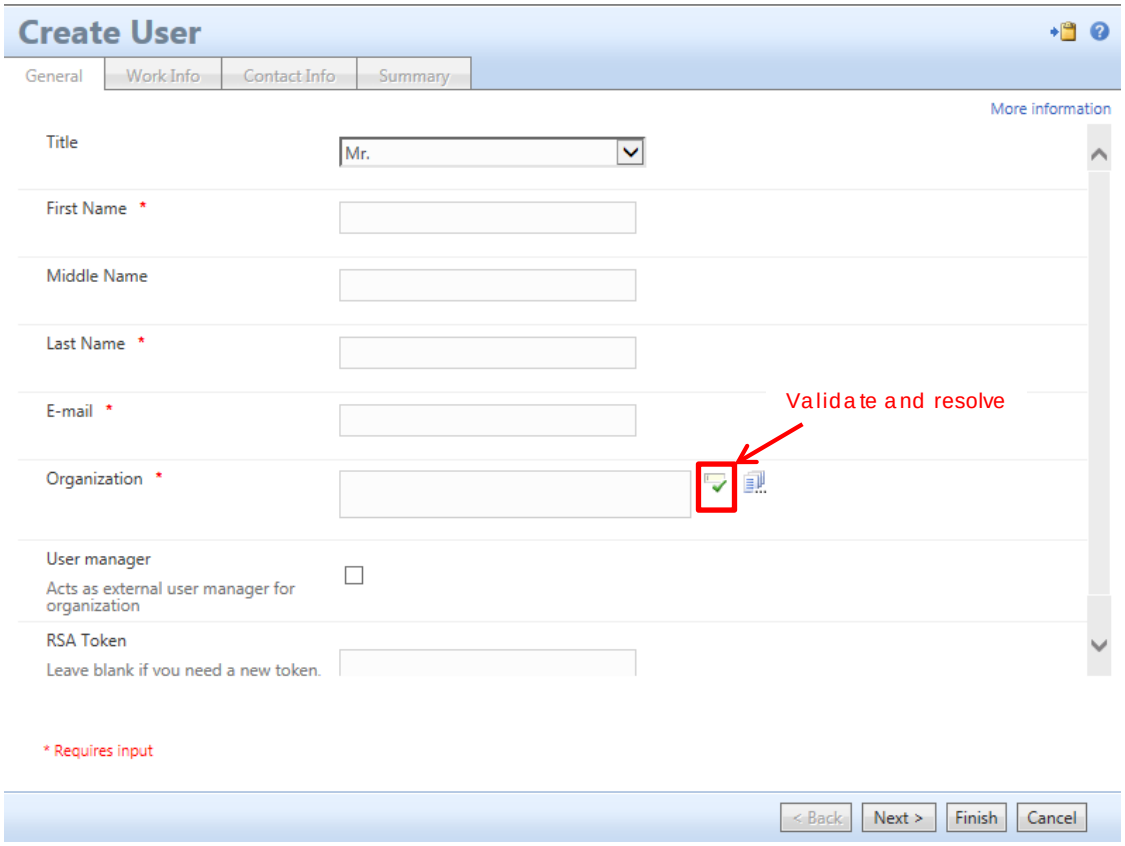

Figure 15: User creation page

Click '**Next'** to launch 'Work Info' page (tab) and the'Contact Info' page (tab). Those can optionally be completed.
Click '**Next'** to launch the last 'Summary' page (tab). Carefully verify the data that was entered in the previous pages.
When all information is verified, click on '**Submit**' to finalise the process.

The **New User** is successfully created.

⚠	If you click on '**Cancel**' in any stage the process is terminated.

4.2 How to search for an existing user

To search for an existing user, select **Account Management** from the left-hand side and in the 'Search for' field type the **name** (FirstName, LastName) or the **UserID** of the user you want to search for.

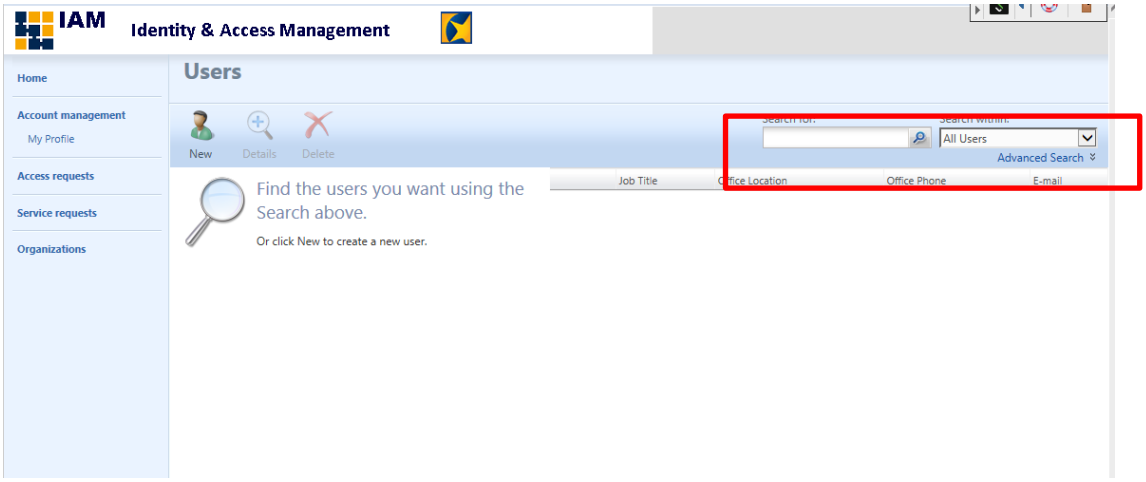

Figure 16: Search for a user

⚠	Leaving the field blank and by clicking on the magnifying lens, the list of all existing users can be retrieved

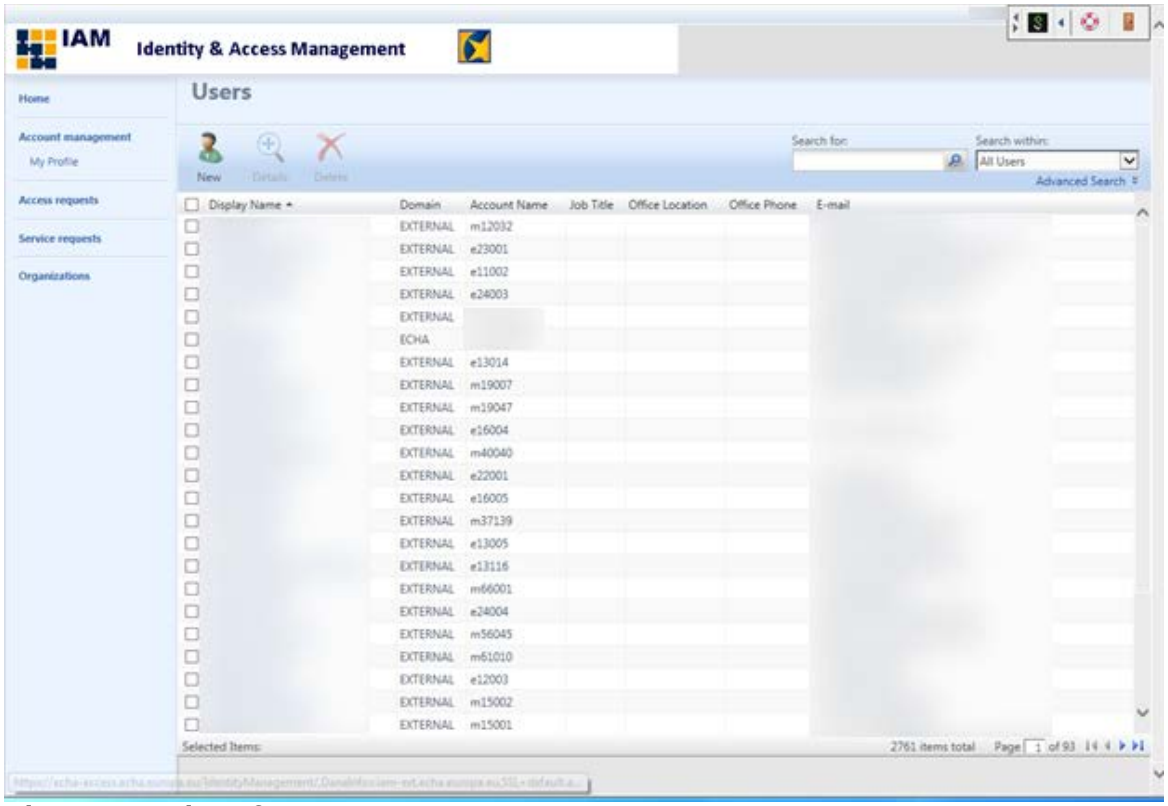

Figure 17: List of Users

4.3 Updating a user profile

From the list of users (Figure 17: List of Userss), select one entry to open the user's information form (Figure 18: User's information form) and update the profile.

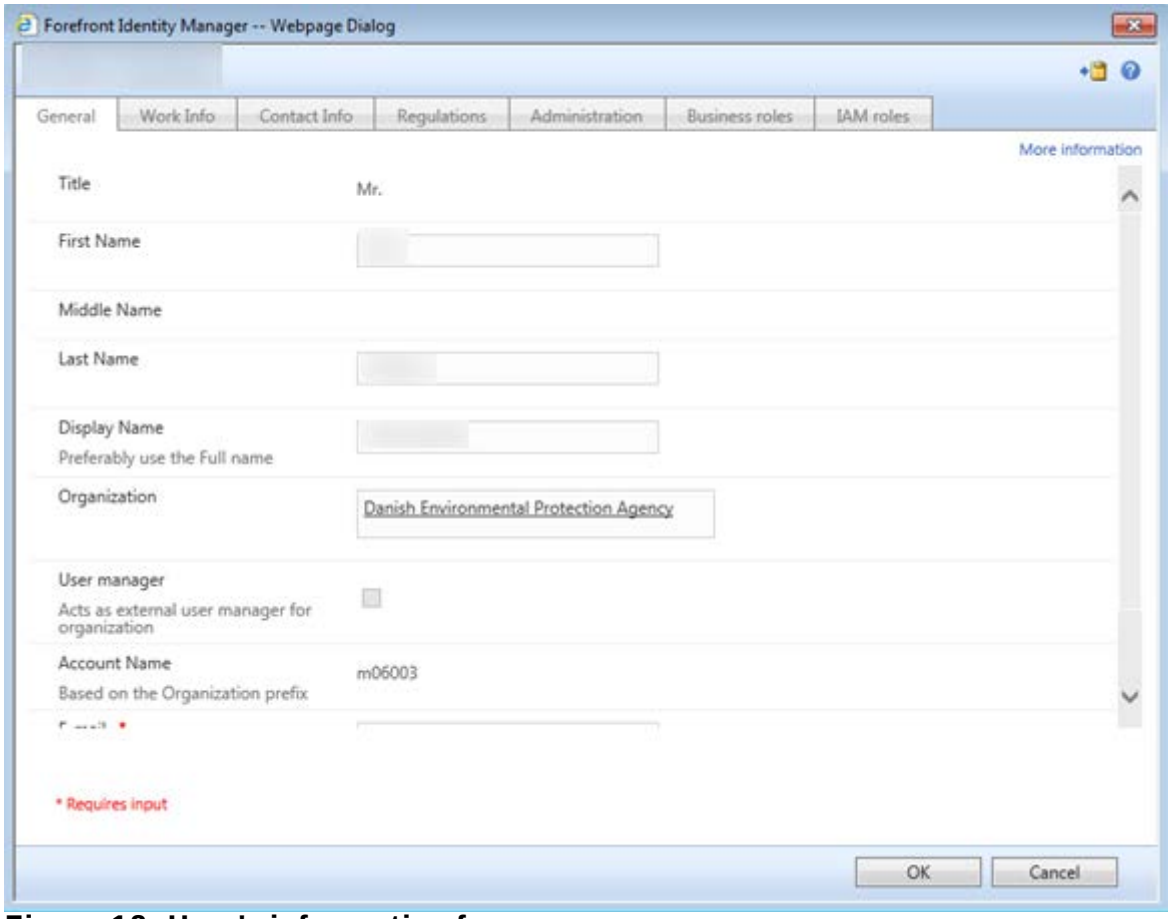

Figure 18: User's information form

Click on '**Submit**' to finalise the process.

4.4 Suspend / Deprovision a user account

For security reasons, the User Administrators can decide to suspend or deprovision an account.

- **Suspend** an account: the account is blocked temporarily. The User Administrator can unblock it if needed.
- **Deprovision** an account: the account is permantly deleted and only the IAM portal team can revoke it.

Suspend

From the list of users (Figure 17: List of Users), select one entry to open the user's information form (Figure 18: User's information form). In the 'Administration' page (tab), check the 'Suspend the account' box. Click on **OK** (Figure 19: Suspend an account). Click on '**Submit**' to finalise the process.

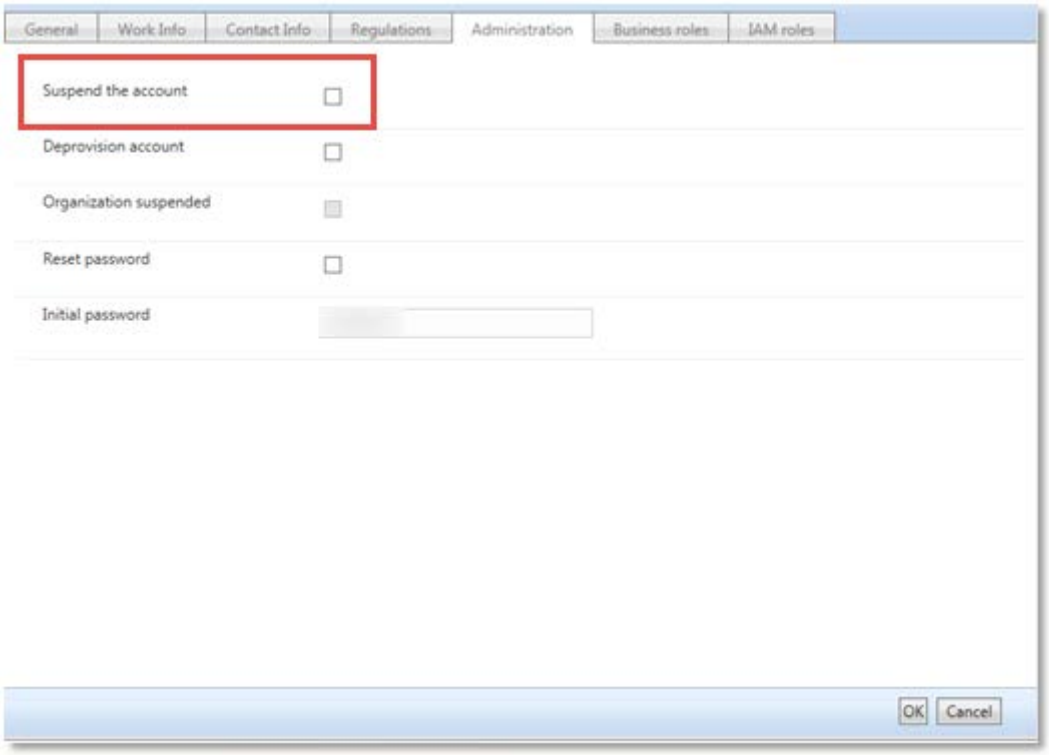

Figure 19: Suspend an account

Deprovision

From the list of users (Figure 17: List of Users), select one entry to open the user's information form (Figure 18: User's information form). In the 'Administration' page (tab), check the 'Deprovision account' box. Click on **OK** (Figure 20: Deprovision an account). Click on '**Submit'** to finalise the process.

⚠	Due to its impact, use the functionality of *Deprovision* with care. Remember that the account is permanently deleted!

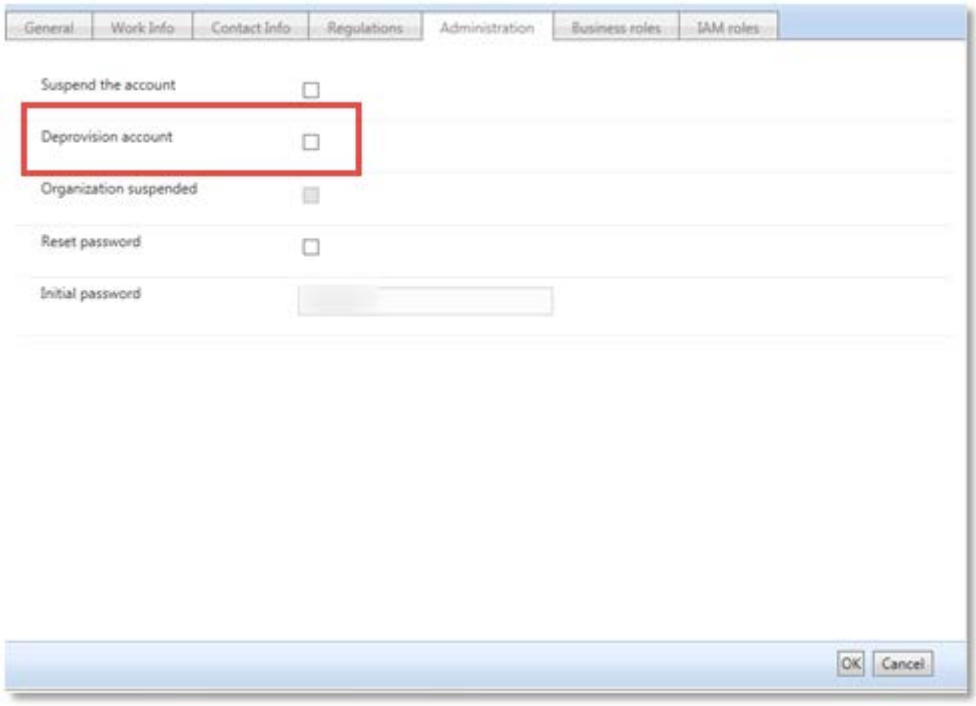

Figure 20: Deprovision an account

4.5 Unblock a user

To unblock a user's account, select **Account Management** from the left-hand side and find the user (Process 6.2). Click on the user. In the '**Administration**' page (tab), uncheck the '**Suspend the account**' box (Figure 19: Suspend an account).
Click on **OK** and then '**Submit**'.

4.6 Resetting a user's password

To perform a password reset, select Account Management from the left-hand side and find the user (Process 6.2). Click on the user. In the 'Administration' page (tab), check the 'Reset Password' box (Figure 21: Password reset). Click on OK and then 'Submit'.

The new initial password appears in the User's Information form (Figure 18: User's information form), in the 'Administration' tab.

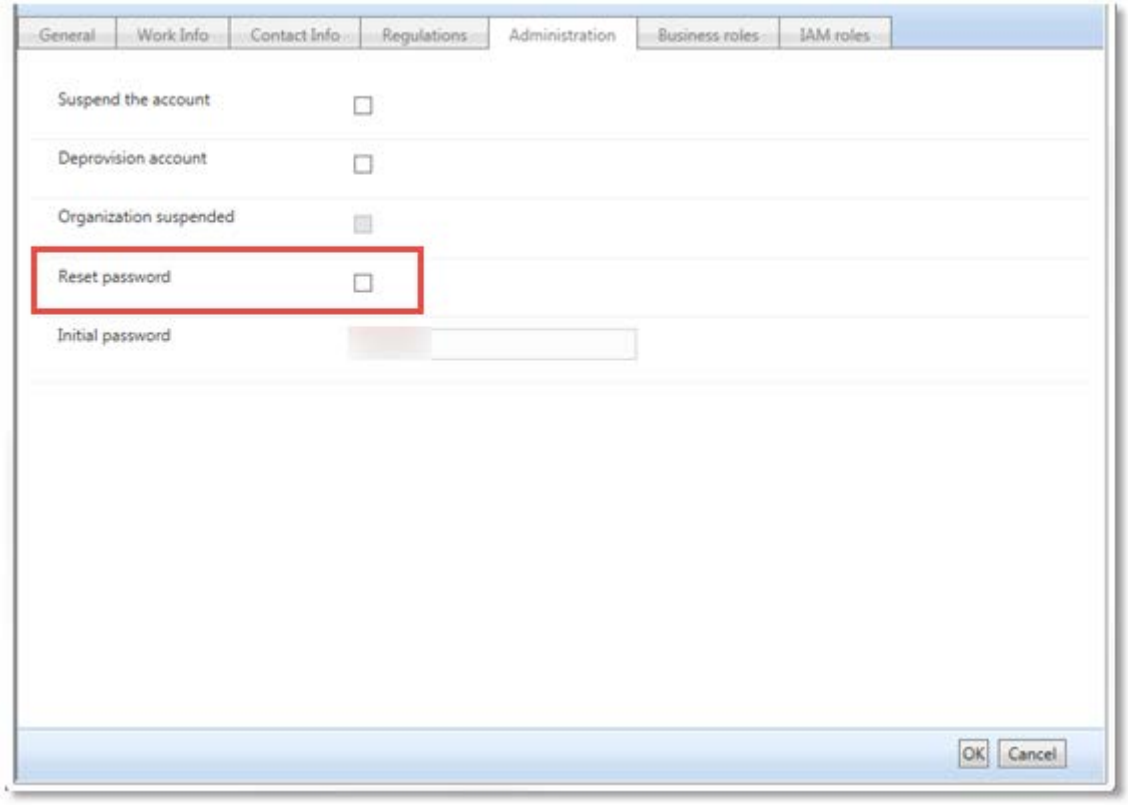

Figure 21: Password reset

5. Access Requests

5.1 Access Request (provision/deprovision a business role)

The User Administrators can place new access request on behalf of the user in their organization to join/leave a business role.

The following list provides an overview of the available Business roles, applications and application roles' description.

	Business Role	Application	Application roles description
1	**NEA PD Auditor**	Interact Portal	NEA PD Auditor is a role used for NEA Auditor. The NEA Auditor collects the Audit Reports from Auditors and investigates audit records in case of data leaks (see the PD-NEA Audit Guideline). The PD NEA Auditor can view audit records in the application and use messaging to a limited extent.
2	**NEA PD FocalPoint**	Interact Portal	PD NEA Focal Point is role used for facilitating communication between ECHA and NEAs. This is the role given to MS Focal Points who coordinate interinstitutional interlinks related to enforcement. In PD NEA they have access to messaging, view news feed and help files.
3	**NEA PD Inspector**	Interact Portal	PD NEA Inspector is a most common role. It is used for inspectors in national enforcement authorities who need to access data submitted to ECHA. They can perform searches, view contents of dossiers dossier, access screening reports, help files and messaging.
4	**NEA ePIC inspector**	ePIC	Read-only access to all the fully processed data in the system, across all MS (with the exception of data related to Article 10 reporting)
5	**MSCA PIC standard**	ePIC	Full processing rights for DNA tasks within the MS (e.g. check export notification, check waiver, register explicit consent request/response, check Article 10 report) and read-only access to all data across all MS
6	**MSCA REACH standard**	IUCLID6	(1) Create Annotations, Read access to all relevant information, dossier creation, print, generate report and executing the validation assistant.

		Interact Portal	(2) Simple and advanced search, simple view, activity pages, Substance report, stored queries, favourites elements, News Feed and Home page customisations.
		REACH-IT	(3) Searching and viewing rights for all dossier types from all countries (global search and reference number search), except for PPORD dossiers, which are country-specific, searching and viewing rights for annotations, Pre-SIEF, pre-registrations, joint submissions, notified substances, companies, internal messages, legal entity changes and C&L submissions; dossier download requests;invoice download requests;EC inventory download;user update rights; submission rights for Annex XV dossiers.
7	**MSCA BPR standard**	IUCLID6	(1) Create Annotations, Read access to all relevant information, dossier creation, print, generate report and executing the validation assistant.
		R4BP 3	(2) View, Edit, Claim, release, assign tasks, initiate ad-hoc communication, upload and send invoices, export cases, download SPC.
8	**MSCA BPR advanced**	IUCLID6	(1) Create Annotations, Read access to all relevant information, dossier creation, print, generate report and executing the validation assistant. (2) Import, Export relevant information.
		R4BP 3	(3) View, edit, claim, release, assign tasks, initiate ad-hoc communication, upload and send invoices, export cases, download SPC.
9	**EC BPR basic**	R4BP	(1) View tasks, preview SPC, Download SPC, Download SPC as PDF
		IUCLID6	(2) Read-only & Print, Export, Import & Create Annotations in IUCLID.
10	**EC BPR standard**	R4BP 3	(1) View, edit, claim, release and assign COM related task items, conduct decision tasks, approve Active substance, search, export cases, preview SPC, download SPC, download SPC as PDF, initiate ad-hoc communication
		IUCLID6	(2) Read-only & Print, Export, Import & Create Annotations in IUCLID.

11	**PCN Normal**	Poison Centres Notifications	Access to the poison centres notifications, download one or multiple notifications
The following roles are meant only for User Administration purposes (access to the IAM portal – not to the other IT tools)			
12	**NEA Administrator**	IAM Portal	Create/delete users, provision/deprovision business roles and request services for Enforcement users
13	**MSCA user administrator**	IAM Portal	Create/delete users, provision/deprovision business roles and request services for Competent Authorities' users
14	**PCNP user administrator**	IAM Portal	Create/delete users, provision/deprovision business roles and request services for Appointed Bodies

In the Welcome screen (Figure 7: Welcome screen in the IAM portal), select **Access requests** from the left-hand side (Figure 22: Access Request).

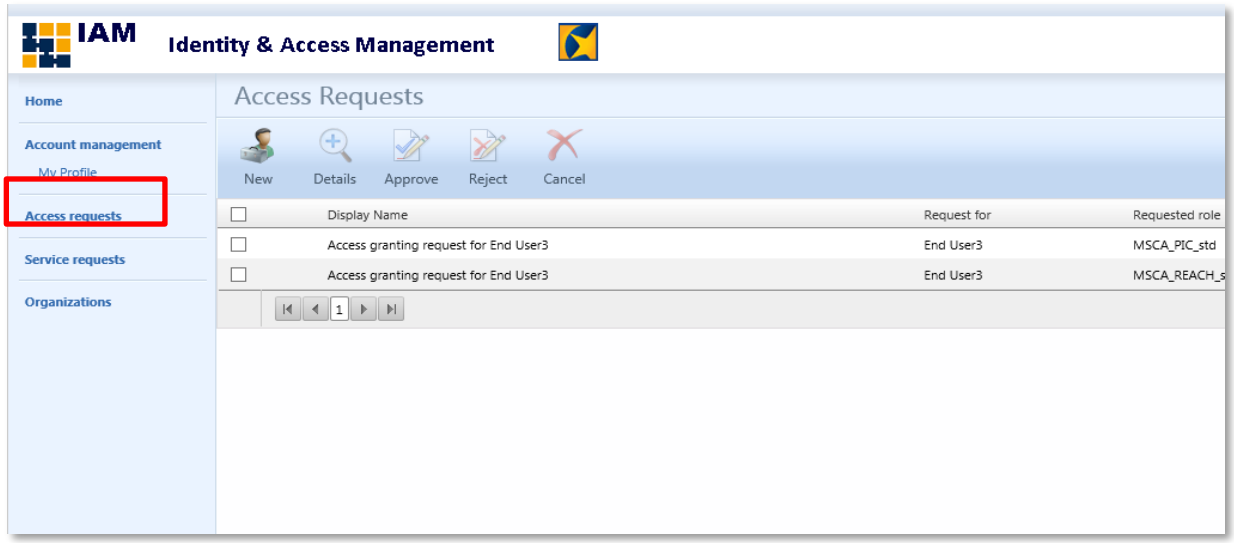

Figure 22: Access Request

Click on 'New' to create a new access request (Figure 23: New Access Request Form).

'Request type': Select either Grand a new business role or Revoke a business role. Fill in the following fields:
'Request for': click on the magnifying lens to choose the user that you are requesting for.

'Requested role': click on the magnifying lens to choose the business role.
'Description': write a small description about the request

Click on '**Save**' to finalise the process.

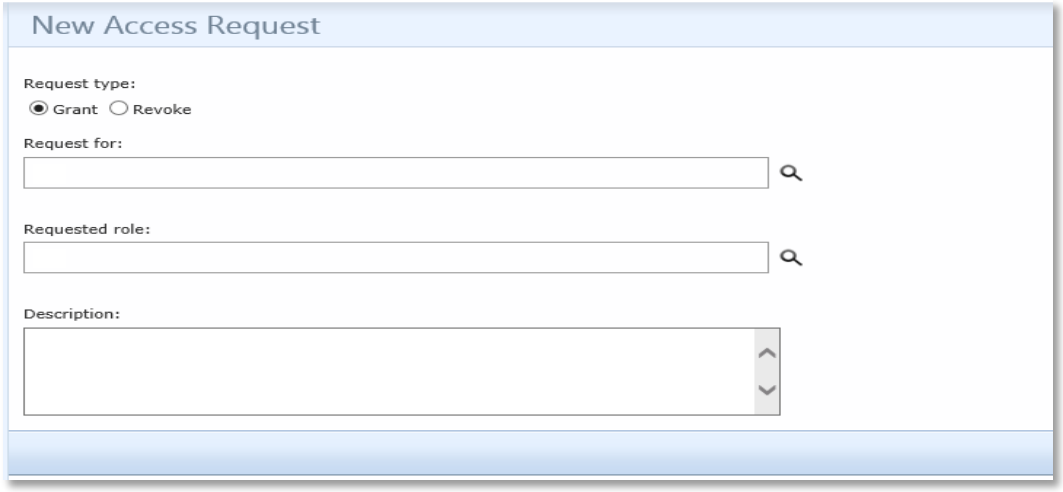

Figure 23: New Access Request Form

⚠	Due to synchronisation between systems, access requests may take up to 24 hours to be completed. If a token management task is also involved, the completion will take longer.

6. Service Requests

6.1 Service Request

The User Administrators can place requests for the services below:

1. RSA token management
2. Users reports in IAM

⚠	Due to synchronisation between systems, service requests may take up to 48 hours to be completed. If a token management task is also involved, the completion will take longer.

In the Welcome screen (Figure 7: Welcome screen in the IAM portal), select **Service requests** from the left-hand side (Figure 24: Service request).

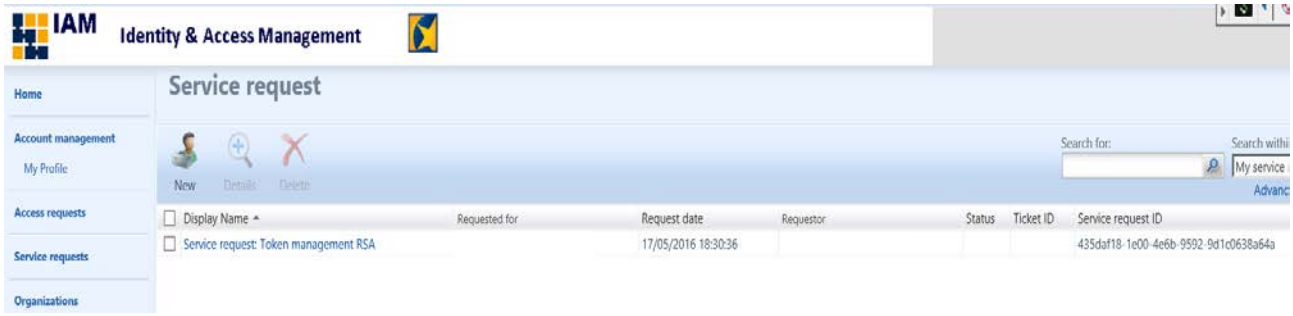

Figure 24: Service request

Click on 'New' to create a new Service request (Figure 25: New Service request).

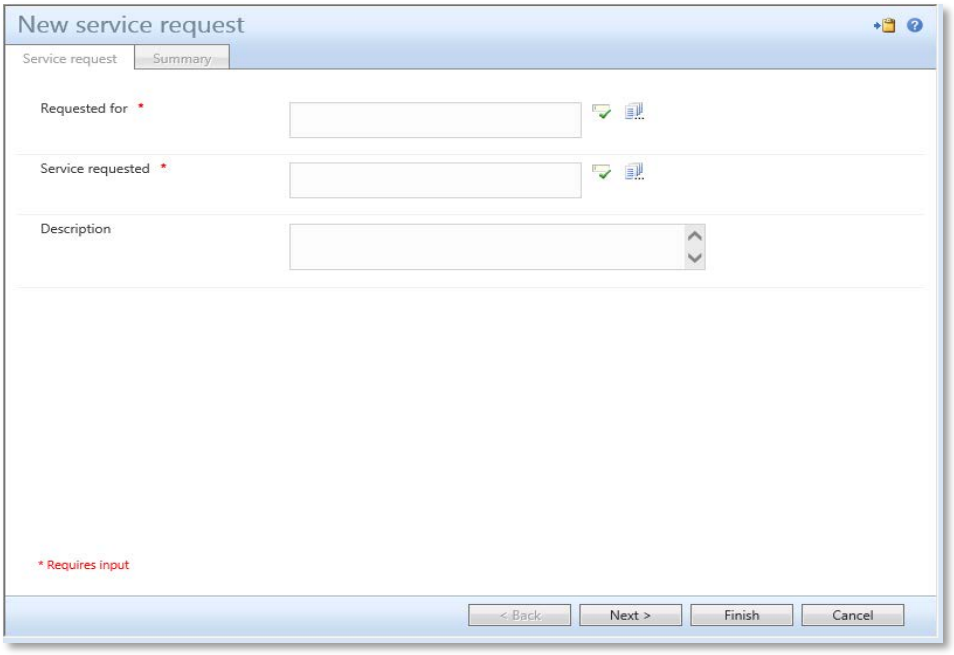

Figure 25: New Service request

'Request for': click on the magnifying lens to choose the user that you are requesting for.
'Service requested': click on the magnifying lens to choose service task. Check the box(es) in the left column to select an action (Figure 26: Select service task).
'Description': write a small description about the request. Click on '**Save**' to finalise the process.

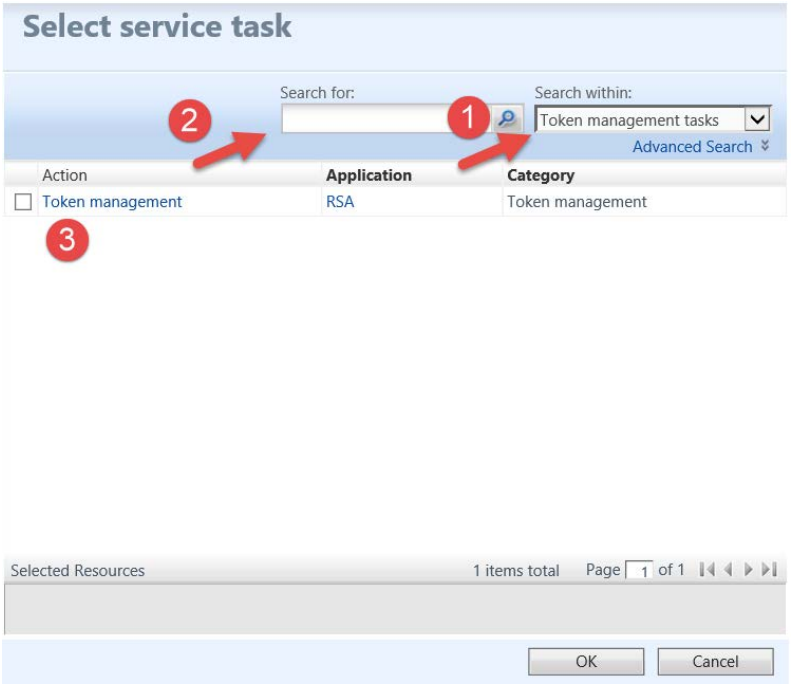

Figure 26: Select service task

7. How to ask ECHA for Support

For technical support or questions related to IAM Portal, use the Authority contact form for National Authorities. It is available on ECHA website, under 'Contact'
https://comments.echa.europa.eu/comments_cms/MSCA_ITsupport_form.aspx

⚠	Use the option 'I need support with IAM portal' to report problems or ask questions regarding the portal. You **should not use** this option for submitting user management requests to ECHA.

Annex

IAM Portal account policies

Below you can find the preconfigured account policies relevant for all End-users.

IAM Portal Account Policies		
Function	**Description**	**Settings**
Account lockout duration	The number of minutes a locked-out account remains locked out before automatically becoming unlocked	120 minutes
Account lockout threshold	The number of failed logon attempts that causes a user account to be locked out	10
Inactivity time out	The time the connection remains open in case of inactivity (a user does not perform any action)	60 minutes
Maximum password age	The period of time (in days) that a password can be used before the system requires the user to change it	180 days
Maximum session time out	The time that the connection remains open in case of active work	8 hours
Minimum password age	The period of time (in days) that a password must be used before the user can change it	1 days
Minimum password length	The least number of characters that a password for a user account may contain	8 characters
Reset account lockout counter after	The number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts	30 inutes

Conventions and terminology

The following icon and terminology are used throughout this manual:

⚠	Very important note

Appointed Body (AB)	Organisations in the Member States responsible for receiving information on the composition of hazardous mixtures in the context of CLP Art. 45, Annex VIII.

BPR	Regulation (EU) No 528/2012 of the European Parliament and of the Council of 22 May 2012 concerning the making available on the market and use of biocidal products
CLP	Regulation (EC) No 1272/2008 on the classification, labelling and packaging of substances and mixtures
COM	European Commission
DNAs	Designated National Authorities
End-Users	Staff members from National organisations that use ECHA IT tools (no User Administrator priviledges)
IAM	Identity Access Management
MSCA	Member State competent authorities
NEA	National Enforcement Authority
OTP	One-time password
PIC	Prior Informed Consent Regulation (Regulation (EU) 649/2012)
R4BP 3	Register for Biocidal Products, version 3, established and maintained by ECHA
REACH	Regulation (EC) No 1907/2006 of the European Parliament and of the council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals
RSA token	SecurID, now known as RSA SecurID, is a mechanism developed by Security Dynamics (later RSA Security, and now RSA) for performing two factor authentication for a user to a network resource
SSL VPN	Secure Sockets Layer virtual private network (i.e. ECHA Remote Access Portal)
Token PIN	Personal Identification Number of the token
User Administrator	Nominated person from national authorities who administers the end users of his/her organisation and is the contact point between his/her organisation users and ECHA in regards to user management
UserID	Username and unique identifier of users. The userID follows the format mXXZZZ for Competent Authorities or eXXZZZ for Enforcement Authorities (XX is the country code and ZZZ the number of the user)

EUROPEAN CHEMICALS AGENCY
ANNANKATU 18, P.O. BOX 400,
FI-00121 HELSINKI, FINLAND
ECHA.EUROPA.EU