

Identity and Access Management (IAM) Portal User Manual

For the nominated User Administrators at national authorities

November 2020

ABC

Disclaimer

This document aims to assist users in complying with their obligations under the REACH Regulation. However, users are reminded that the text of the REACH Regulation is the only authentic legal reference and that the information in this document does not constitute legal advice. Usage of the information remains under the sole responsibility of the user. The European Chemicals Agency does not accept any liability with regard to the use that may be made of the information contained in this document.

Version	Changes	
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
1.4	Business role update (MSCA REACH advanced), minor editorial changes	August 2019
1.5	Reporting Functionality and minor editorial changes	November 2019

Identity and Access Management (IAM) Portal User Manual

Reference: ECHA-20-H-22-EN

ISBN: 978-92-9481-727-3

Cat. Number: ED-01-20-680-EN-N

DOI: 10.2823/197317

Publ.date: November 2020

Language: EN

© European Chemicals Agency, 20xx
Cover page © European Chemicals Agency

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/contact>

European Chemicals Agency

Mailing address: P.O. Box 400, FI-00150 Helsinki, Finland
Visiting address: Telakkakatu 6-8, Helsinki, Finland

Table of Contents

1. Introduction	5
1.1 Scope and pre-conditions	5
1.2 What can I do in IAM Portal?.....	5
2. ECHA Remote Access Portal	6
2.1 Login to the IAM Portal.....	6
2.2 First time login to ECHA Remote Access Portal	8
3. IAM Portal	11
3.1 Login to the IAM Portal.....	11
3.2 First time Login to IAM Portal.....	9
3.3 IAM password reset and change functionality	12
4. Account Management	14
4.1 Creating a new user account.....	14
4.2 How to search for an existing user.....	15
4.3 Updating a user profile.....	17
4.4 Suspend/ Deprovision a user account.....	17
4.5 Unblock a user	19
4.6 Resetting a user's password.....	19
5. Access Requests	21
5.1 Access Request (provision/deprovision a business role)	21
6. Service Requests	26
6.1 Service Request	26
7. Organization Information report	28
7.1 Login to the Organization Information Report.....	28
7.2 Generating a new report	28
8. How to ask ECHA for Support	30
Annex	31
IAM Portal account policies.....	31
Conventions and terminology	31

Table of Figures

Figure 1: ECHA Remote Access Portal Login page	6
Figure 2: ECHA Remote Access Portal Login page – Web Bookmarks	7
Figure 3: Tokencode	8
Figure 4: Setting a new Personal Identification Number (PIN)	8
Figure 5: ECHA Remote Access Portal Login page – PIN set successfully	9
Figure 6: ECHA Remote Access Portal Login page – Bookmarks: IAM Portal	11

Figure 7: Welcome screen in the IAM portal	11
Figure 8: IAM Portal Activation and Password reset Login page	9
Figure 9: IAM Portal Activation – changing OTP step 1	10
Figure 10: IAM Portal Activation – changing OTP step 2	10
Figure 11: IAM Portal Activation – changing OTP step 3	11
Figure 12: IAM Portal Activation – changing OTP step 4	11
Figure 13: IAM Portal Activation and Password reset – Reset and change functionalities.....	12
Figure 14: Create a New User	14
Figure 15: User creation page	15
Figure 16: Search for a user	16
Figure 17: List of Users	16
Figure 18: User's information form	17
Figure 19: Suspend an account	18
Figure 20: Deprovision an account.....	19
Figure 21: Password reset	20
Figure 22: Access Request	24
Figure 23: New Access Request Form	25
Figure 24: Service request	26
Figure 25: New Service request	26
Figure 26: Select service task	27

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 VPN¹ 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 Administrators 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.

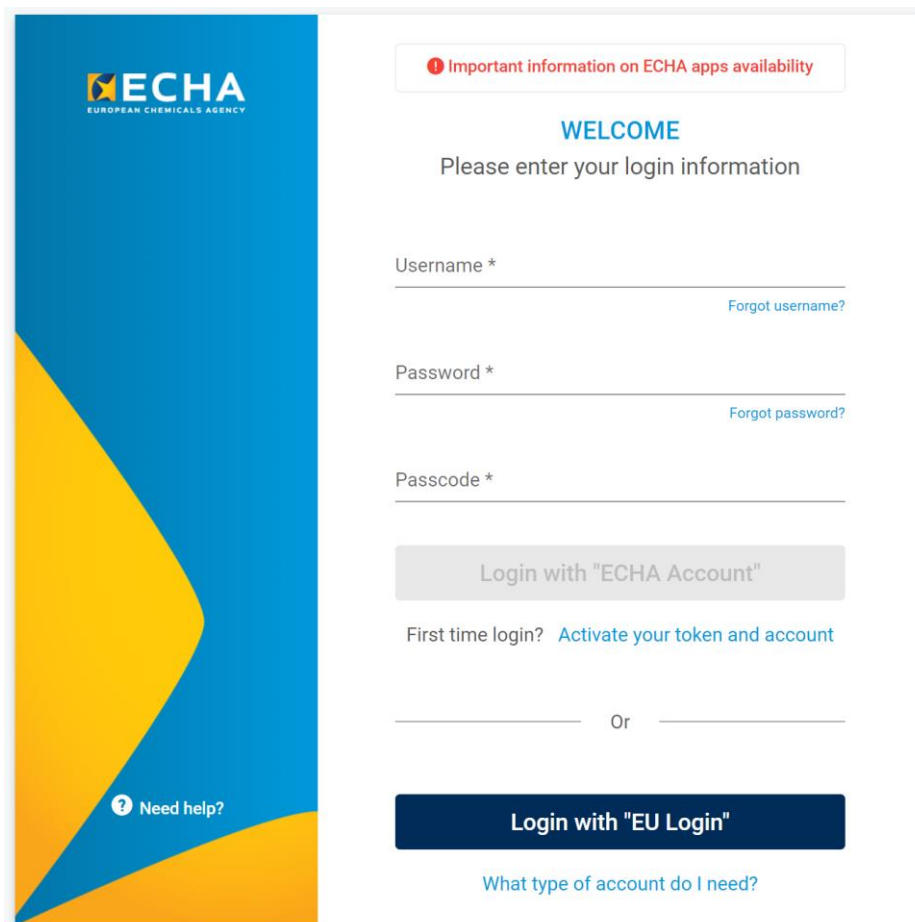
2. ECHA Remote Access Portal

	If this is the first time you are accessing ECHA Remote Access Portal, check first section 2.2 First time login
---	---

2.1 Login to the IAM Portal

Access ECHA Remote Access Portal via <https://vpn.echa.europa.eu/eulogin> (Figure 1)

- In the field 'Username', type your userID
- In the field Password, type your password
- In the field 'Passcode' type your PIN followed by Tokencode in your RSA token (figure 3) and click 'Login with "ECHA Account"'



Important information on ECHA apps availability

WELCOME
Please enter your login information

Username * [Forgot username?](#)

Password * [Forgot password?](#)

Passcode *

Login with "ECHA Account"

First time login? [Activate your token and account](#)

Or

Login with "EU Login"

[What type of account do I need?](#)

[Need help?](#)

Figure 1: ECHA Remote Access Portal secure 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). Please note that the bookmarks could be appearing different depending on the effective roles each IAM User Administrator has.

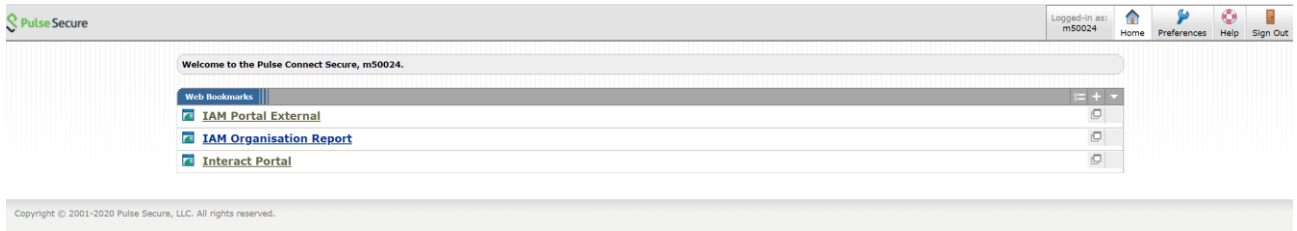


Figure 2: ECHA Remote Access Portal Login page – Web Bookmarks

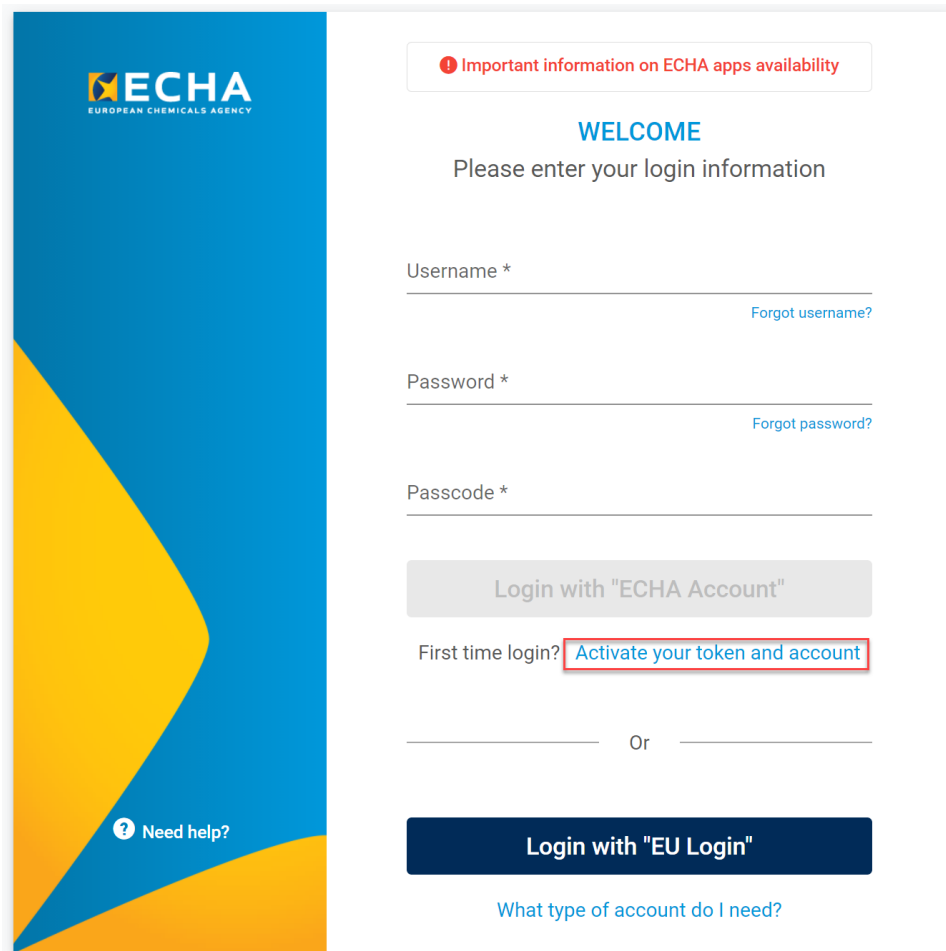
2.2 First time login – how to activate your token and account

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://vpn.echa.europa.eu/eulogin>
- Click the link "Activate your token and account" (figure 4)
- Follow the 4 steps to activate your token and account (figure 5)



Figure 3: Tokencode



ECHA
EUROPEAN CHEMICALS AGENCY

Important information on ECHA apps availability

WELCOME
Please enter your login information

Username * [Forgot username?](#)

Password * [Forgot password?](#)

Passcode *

Login with "ECHA Account"

First time login? [Activate your token and account](#)

Or

Login with "EU Login"

[What type of account do I need?](#)

[Need help?](#)

Figure 4: Activate your token and account

- Step1: Insert your username and email and press next

Activate your account

1 Enter username and email — 2 Setup Token PIN — 3 Enter OTP — 4 Setup Password

USER INFORMATION
Enter your username and email address. Please do not interrupt the process without completing all four steps

Username *
example-user

Email *
example@echa.europa.eu

Cancel Next

Figure 5: Steps to Activate your token and account – Step 1

- Step 2: Enter the token code and new PIN twice and press “Next”

Activate your account

✓ Enter username and email — 2 Setup Token PIN — 3 Enter OTP — 4 Setup Password

TOKEN DEVICE
Set up your Personal Identification Number (PIN) containing 4 to 8 characters

Token Code *
159759
Please enter your tokencode displayed at the hardware token screen 5/6

Token Pin *

Your PIN should be 4 to 8 characters long, not be structured by a set of the same number (e.g 0000) or be a set of consecutive numbers (e.g 1234) 4/8

Confirm Token Pin *
**** 4/8

Cancel Next




Figure 6: Steps to Activate your token and account – Step 2

- Step 3: Enter the OTP as received automatically in your email and press “Next”

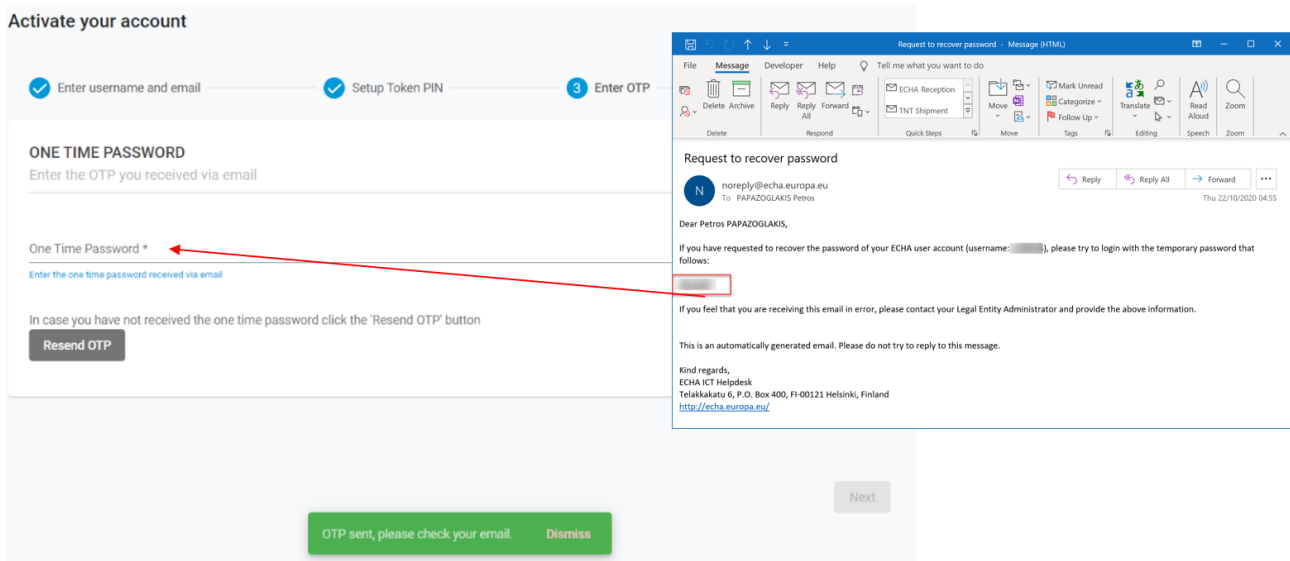


Figure 7: Steps to Activate your token and account – Step 3

- Step 4: Enter your permanent password twice and press “Activate your account” button

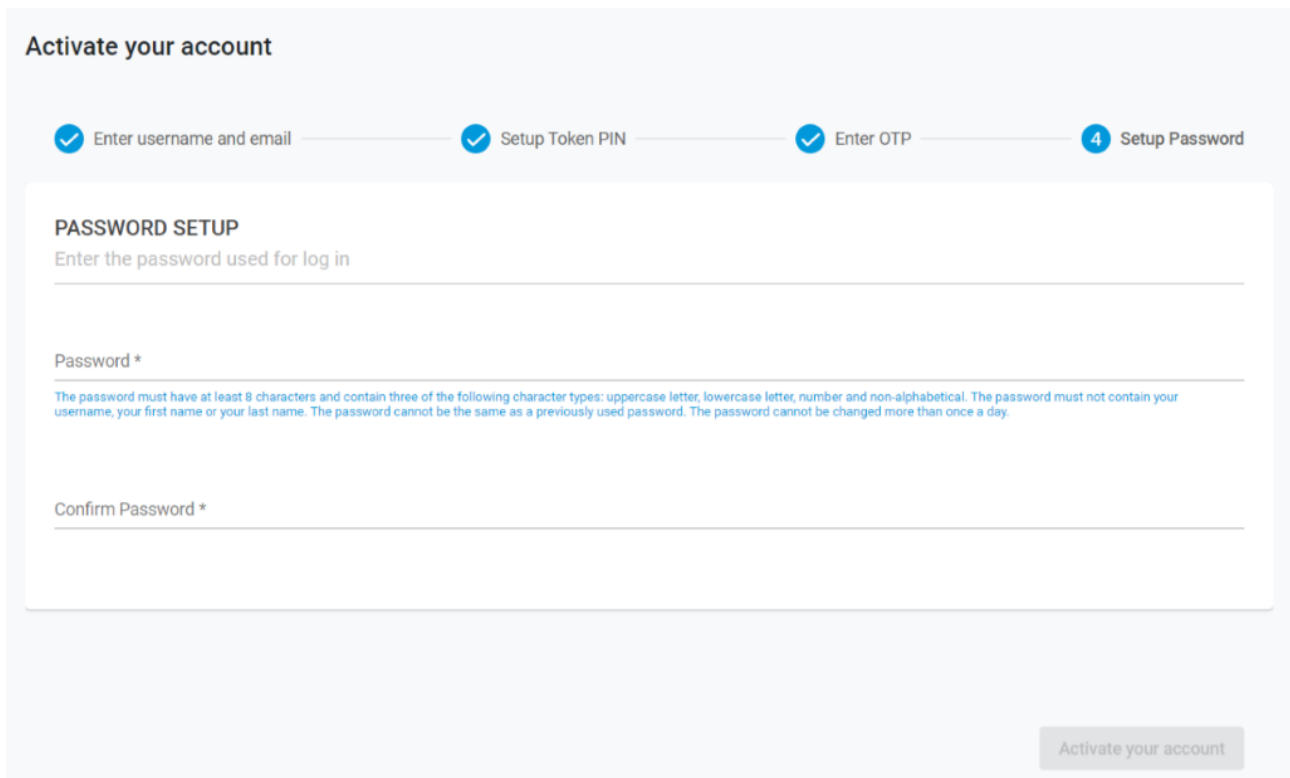


Figure 8: Steps to Activate your token and account – Step 4

Your account and token have been set.

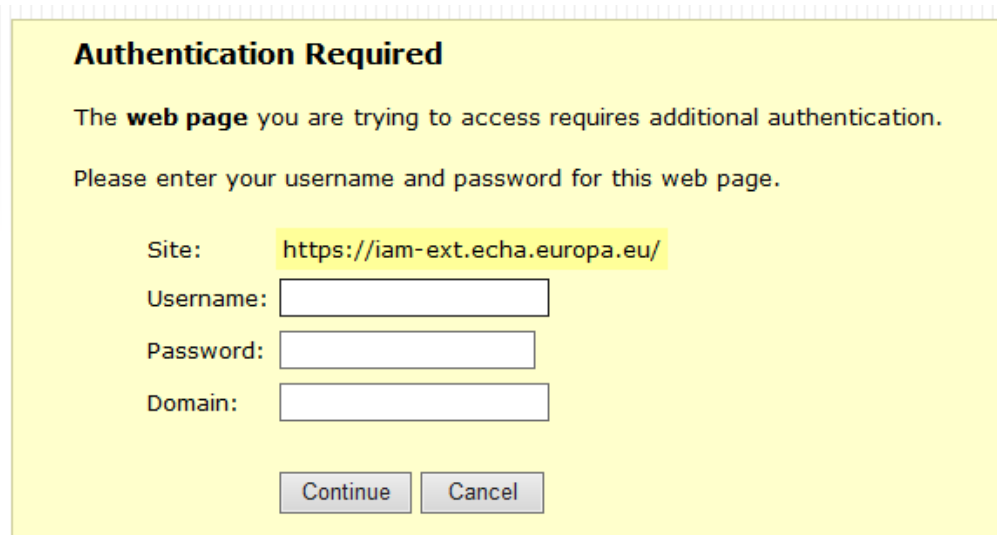
Remember to set a PIN and password that you can easily remember.

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'



Authentication Required

The **web page** you are trying to access requires additional authentication.

Please enter your username and password for this web page.

Site: <https://iam-ext.echa.europa.eu/>

Username:

Password:

Domain:

Figure 9: ECHA Remote Access Portal Login page – Bookmarks: IAM Portal

After logging-in successfully into the IAM Portal, you will be able to see the welcome screen of the portal (Figure 10: Welcome screen in the IAM portal).

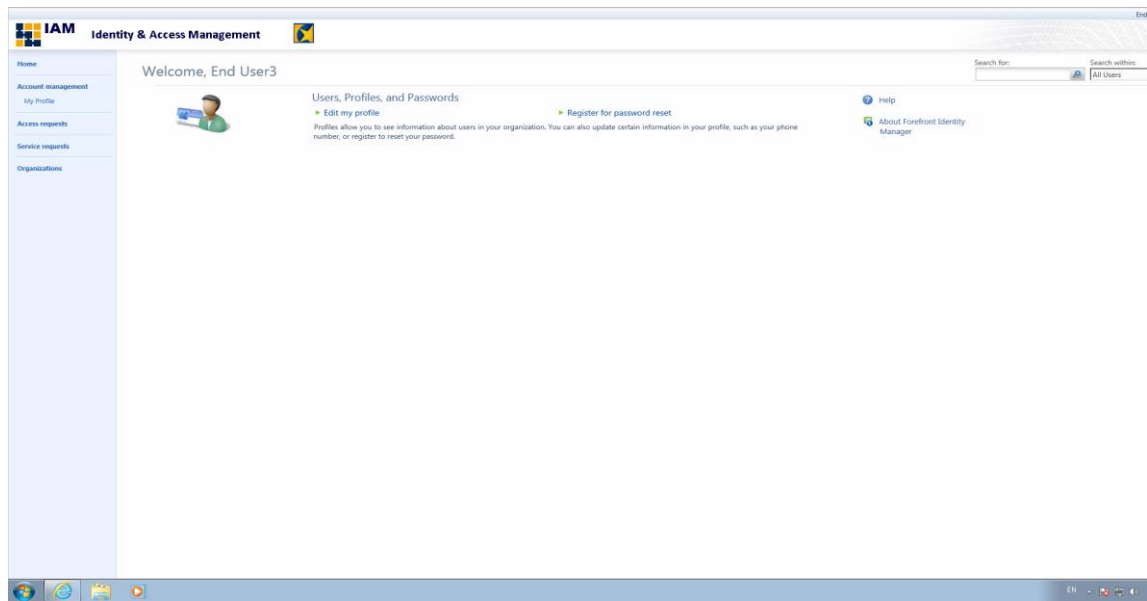
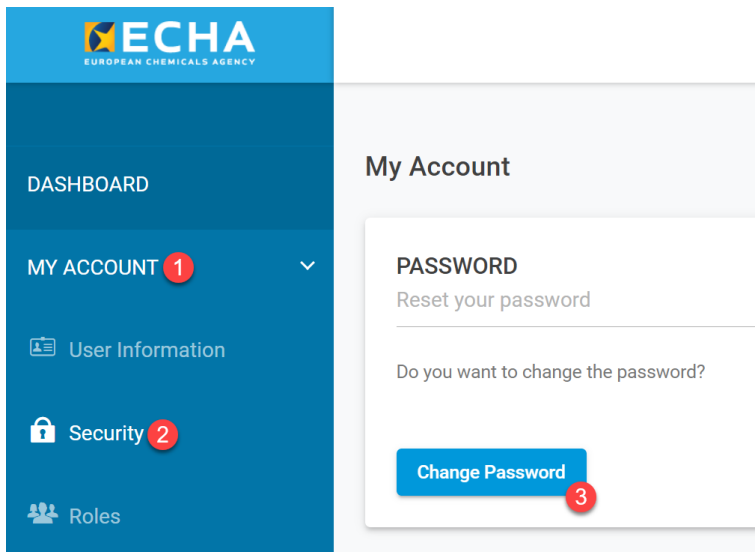



Figure 10: Welcome screen in the IAM portal

3.2 Change, Forgot Password and username functionality

In case you do not remember your username and your password you can use the Forgot username and password functionality (figure 13).

You can also change your password any time but not more than once per day, by visiting the page: <https://idp.echa.europa.eu/ui/secure-login> and follow the below indicated steps below:



	Remember that you can change your password only once a day.
---	---

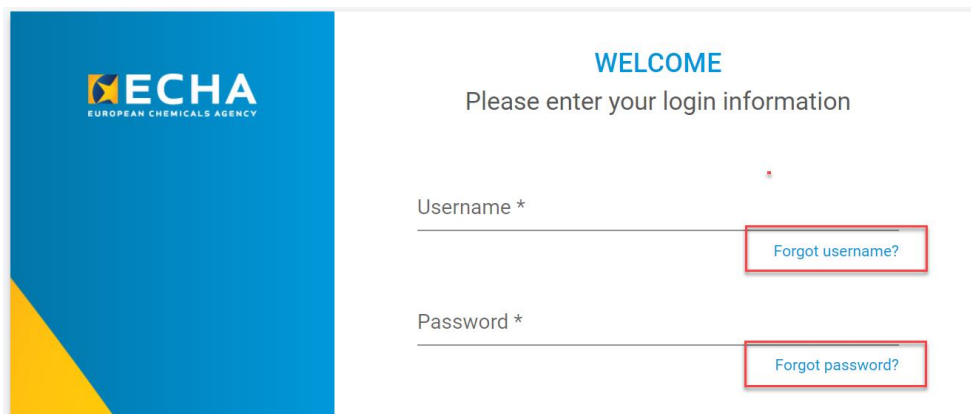


Figure 11: IAM Portal Activation and Password reset – Reset and change functionalities



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 (USERS)** from the left-hand side and then click on 'New'.

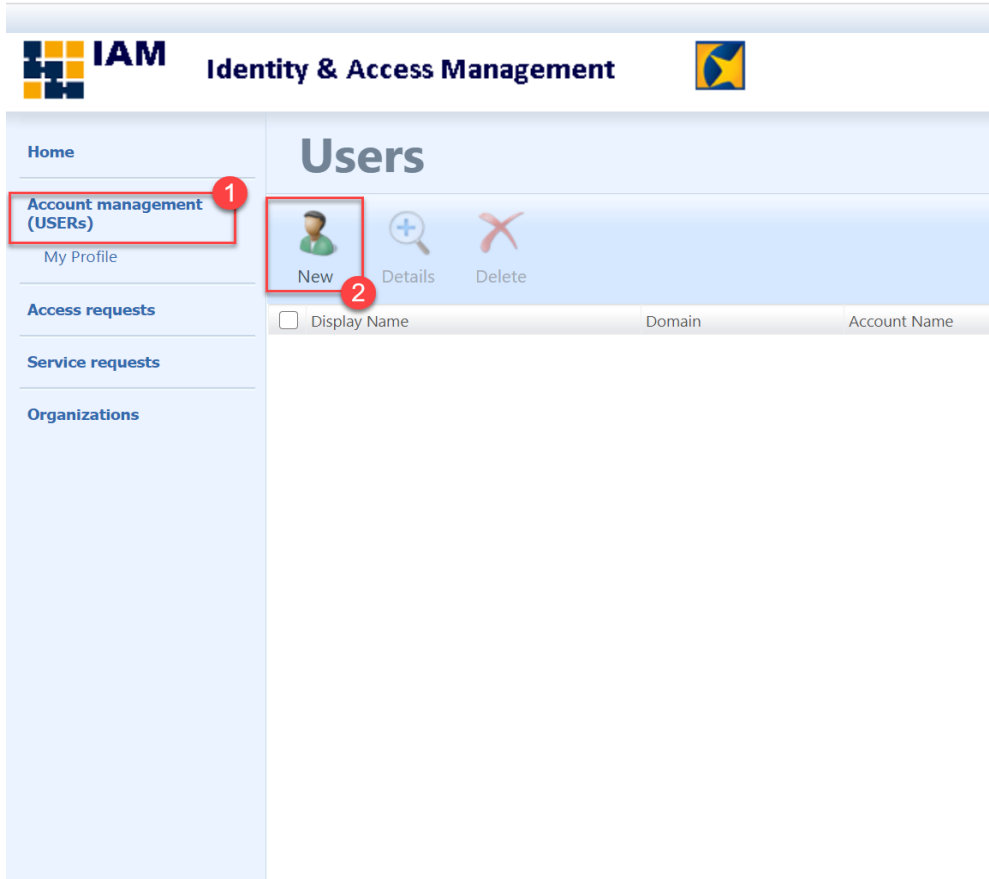


Figure 12: Create a New User

The **Create User** page (

Figure 13:

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. Alternatively, instead of the organization name, use the organization prefix (e.g. m50 – three first characters of each username) or the UUID of the organization (e.g. ECHA-c085d5f3-aa00-4a42-b5a9-0cafac77200d) and then validate it by clicking the green check symbol.

	<p>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.</p>
--	--

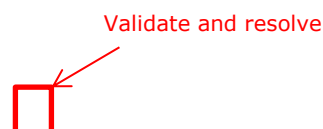


Figure 13: User creation page

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.

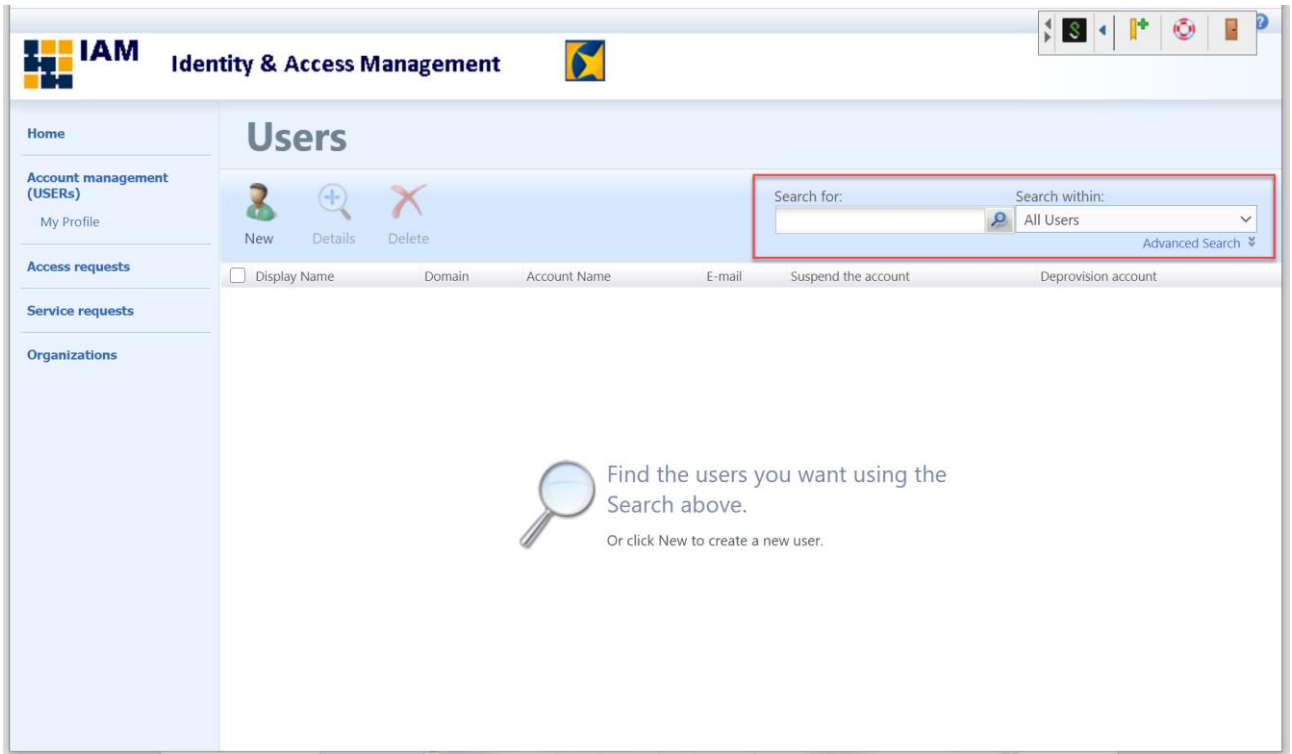



Figure 14: Search for a user

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

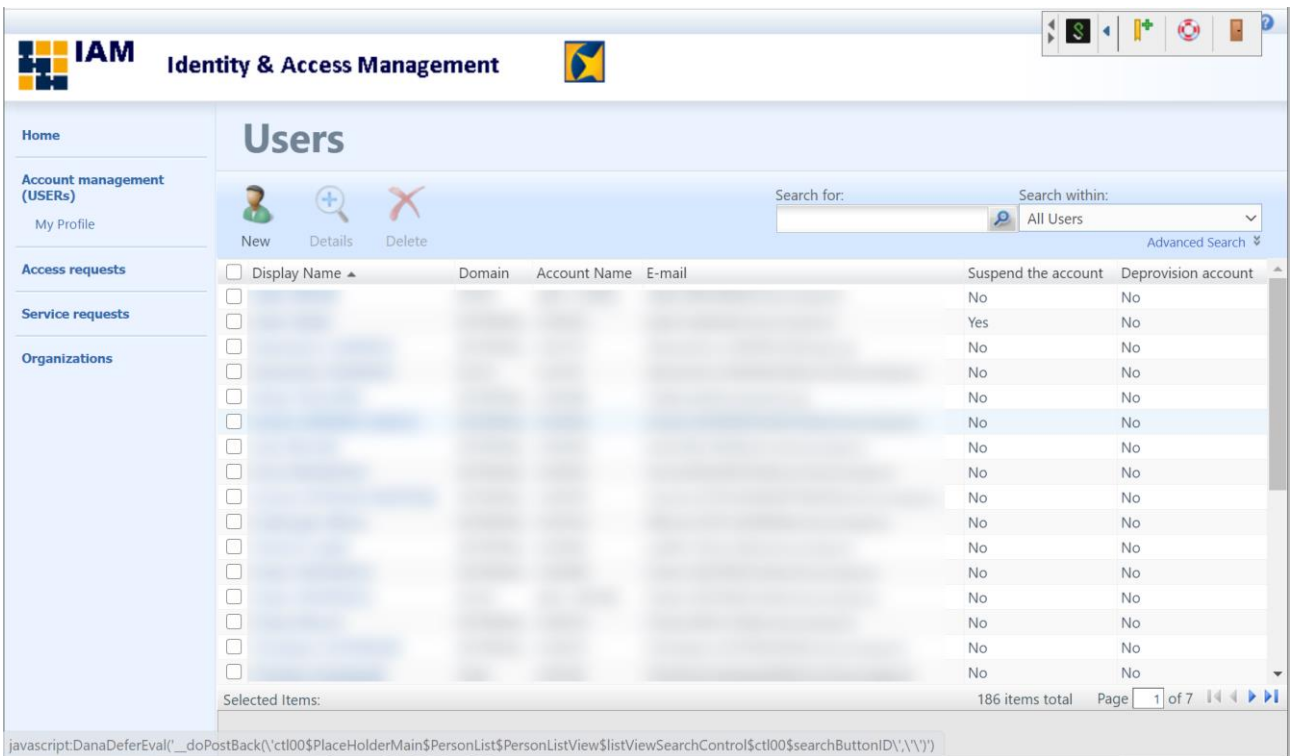


Figure 15: List of Users

4.3 Updating a user profile

From the list of users (Figure 15: List of Userss), select one entry to open the user's information form (Figure 16: User's information form) and update the profile.

The screenshot shows a web-based form for updating a user profile. The form is titled "Admin: REALTIME" and has a tabbed interface with the following tabs: "General", "Work Info", "Contact Info", "Regulations", "Administration", "Business roles", and "IAM roles". The "General" tab is currently selected. The form contains the following fields and controls:

- Title:** Mr.
- First Name:** [Text input field]
- Middle Name:** [Text input field]
- Last Name:** [Text input field]
- Display Name:** [Text input field] with the note "Preferably use the Full name".
- Organization:** [Text input field]
- User manager:** Acts as external user manager for organization. [Checkbox]
- Account Name:** [Text input field] with the note "Based on the Organization prefix".
- E-mail:** [Text input field] with a red asterisk indicating it is required.
- RSA Token (effective):** This value is imported from the RSA configuration.

At the bottom left of the form, there is a red asterisk and the text "* Requires input". At the bottom right, there are "OK" and "Cancel" buttons.

Figure 16: User's information form

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

4.4 Suspend/ Deprovision a user account

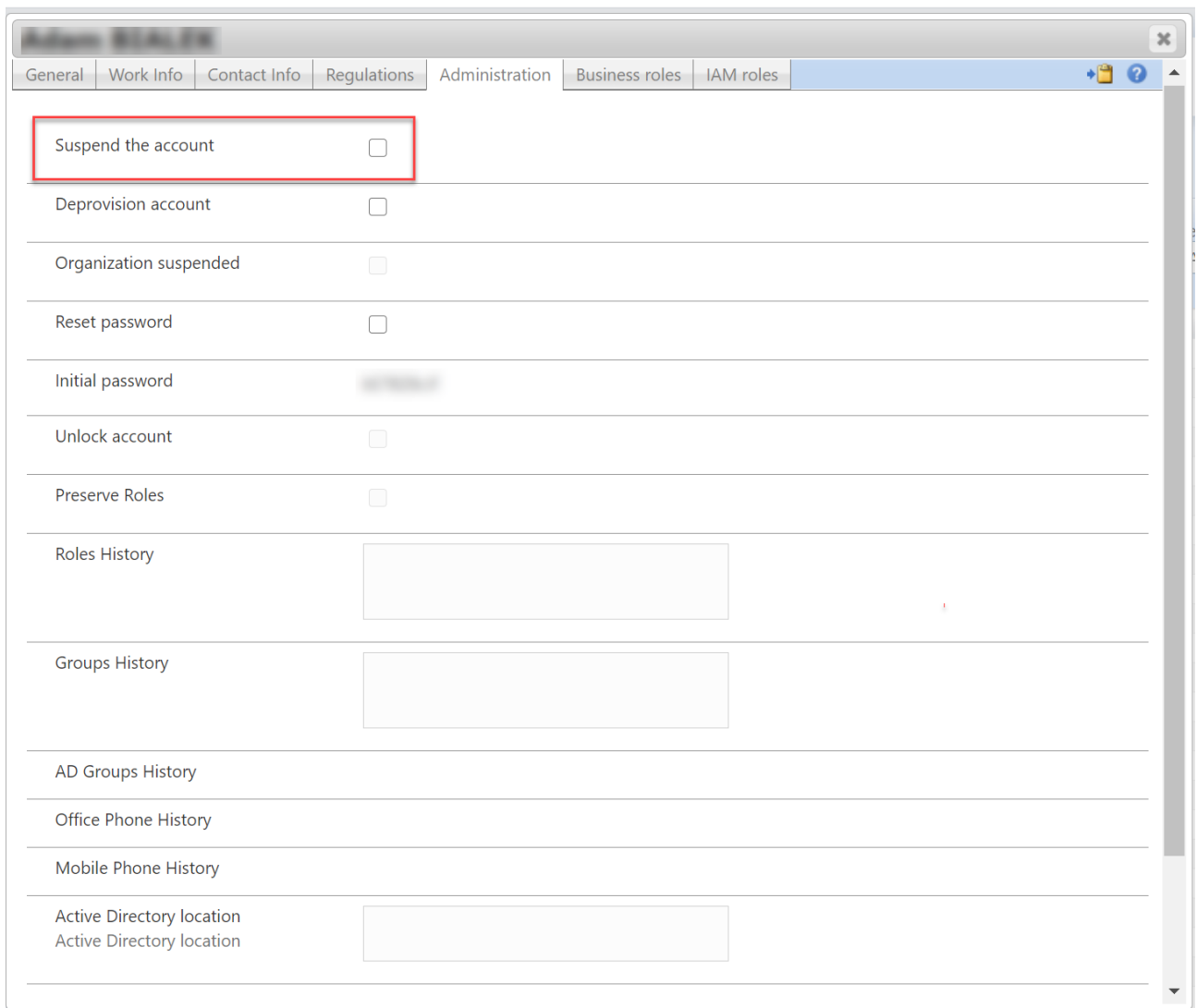
For security reasons, the User Administrators can decide to suspend or deprovision an account.

- **Suspend** an account: the account is blocked temporarily. The User Administrator can unblock it if needed. The roles are retained when account is suspended. If you want them to be removed you must do that before you suspend the account.

- **Deprovision** an account: the account is permanently deleted and only the IAM portal team can revoke it. Also, all the roles are removed from the deprovisioned account.

Suspend

From the list of users (Figure 15: List of Users), select one entry to open the user's information form (Figure 16: User's information form). In the 'Administration' page (tab), check the 'Suspend the account' box. Click on **OK** (Figure 17: Suspend an account). Click on '**Submit**' to finalise the process.



The screenshot shows a web application window titled 'Admin: USER FN'. The 'Administration' tab is selected, and the 'Suspend the account' checkbox is highlighted with a red box. The form contains several other options and history sections:


Suspend the account	<input type="checkbox"/>
Deprovision account	<input type="checkbox"/>
Organization suspended	<input type="checkbox"/>
Reset password	<input type="checkbox"/>
Initial password	*****
Unlock account	<input type="checkbox"/>
Preserve Roles	<input type="checkbox"/>
Roles History	<input type="text"/>
Groups History	<input type="text"/>
AD Groups History	
Office Phone History	
Mobile Phone History	
Active Directory location	<input type="text"/>
Active Directory location	<input type="text"/>

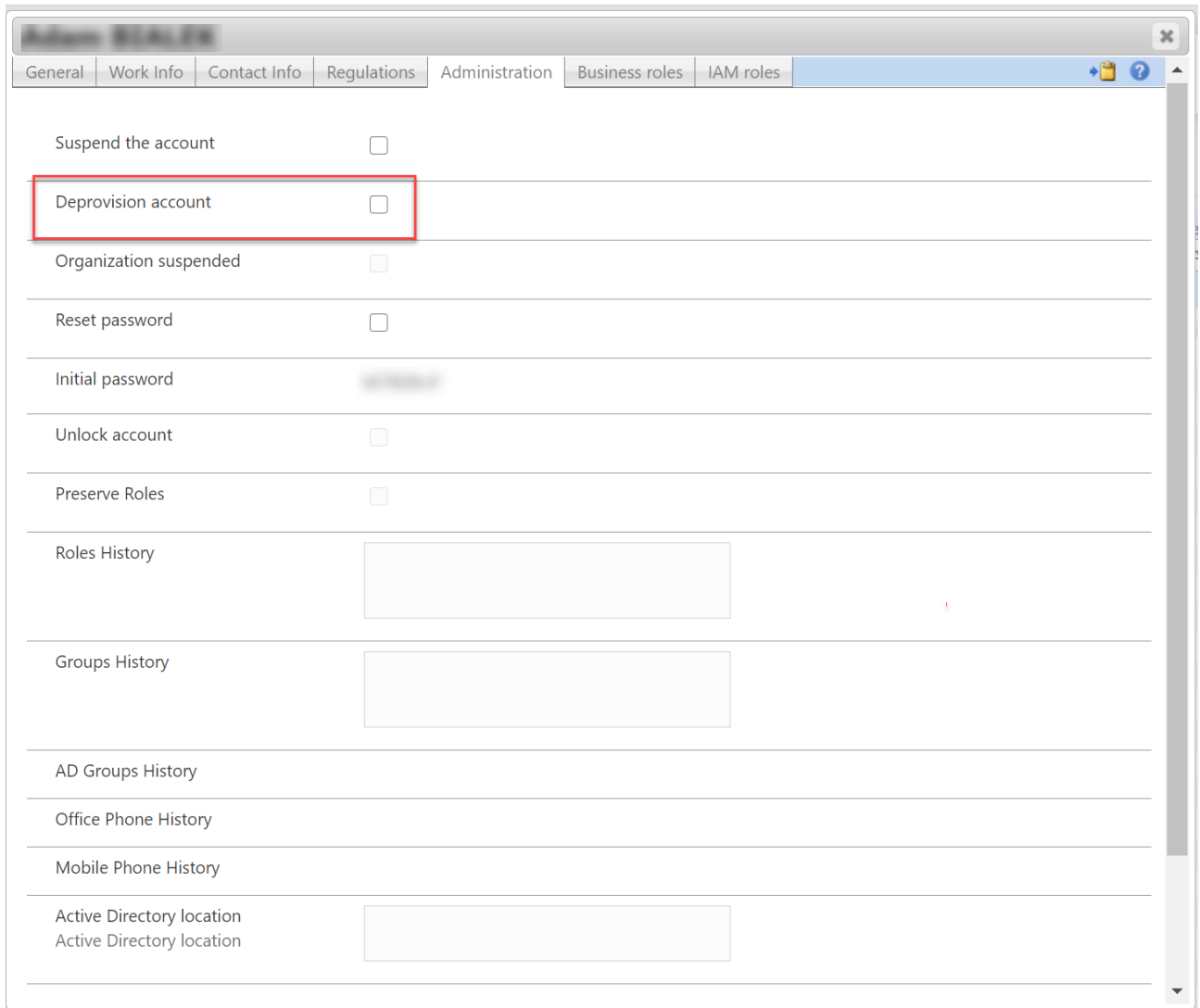
Figure 17: Suspend an account

Deprovision

From the list of users (Figure 15: List of Users), select one entry to open the user's information form (Figure 16: User's information form). In the 'Administration' page (tab), check the 'Deprovision account' box. Click on **OK** (Figure 18: Deprovision an account). Click on '**Submit**'

to finalise the process.

	<p>Due to its impact, use the functionality of <i>Deprovision</i> with care.</p> <p>Remember that the account is permanently deleted!</p>
---	---



The screenshot shows a web interface for user management. At the top, there are tabs: General, Work Info, Contact Info, Regulations, Administration (selected), Business roles, and IAM roles. Below the tabs, there is a list of actions with checkboxes:

- Suspend the account
- Deprovision account** (highlighted with a red box)
- Organization suspended
- Reset password
- Initial password
- Unlock account
- Preserve Roles
- Roles History
- Groups History
- AD Groups History
- Office Phone History
- Mobile Phone History
- Active Directory location
- Active Directory location

Figure 18: Deprovision an account

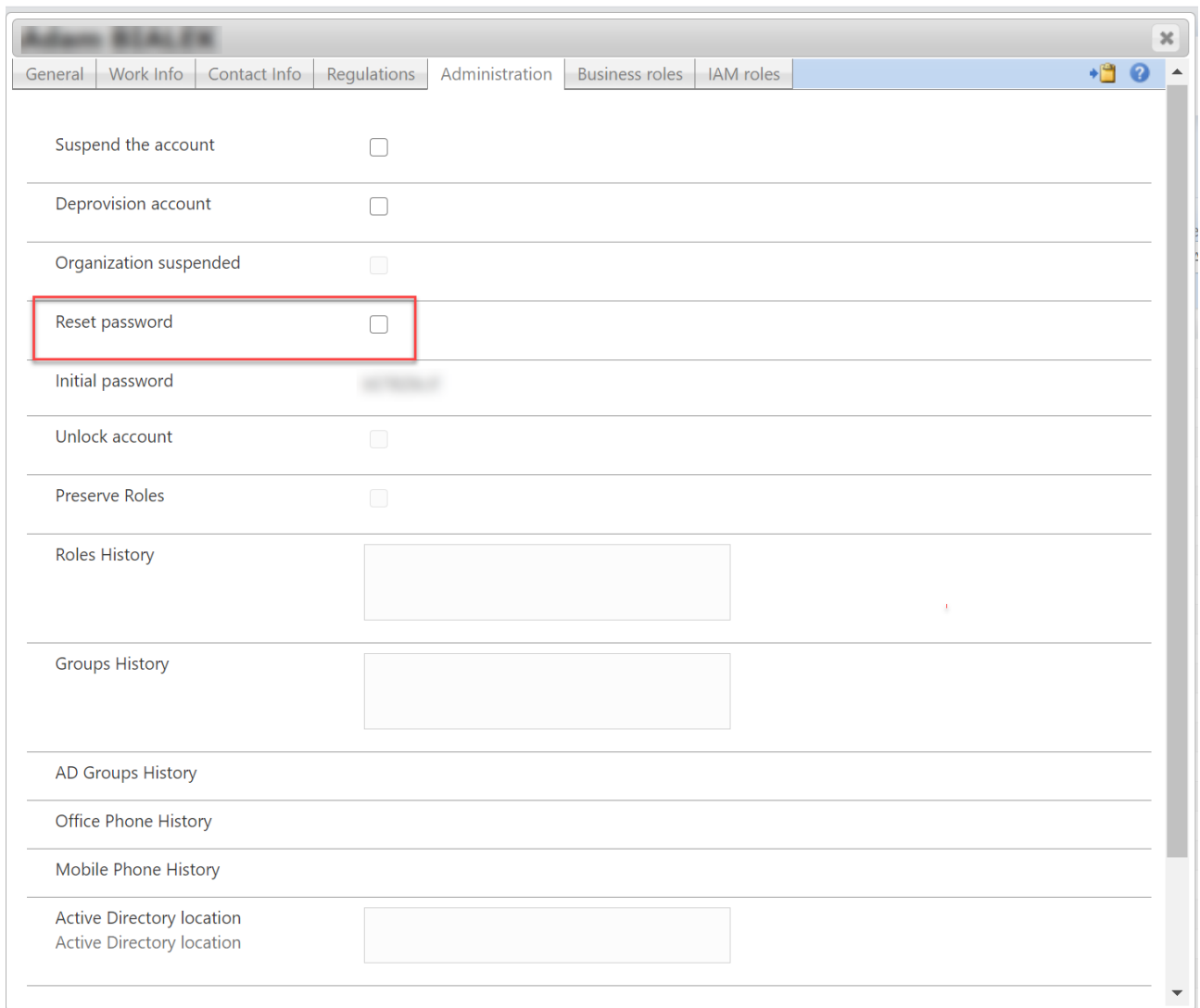
4.5 Unblock a user

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 17: 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 19: Password reset). Click on OK and then 'Submit'.

The new initial password appears in the User's Information form (Figure 16: User's information form), in the 'Administration' tab.



The screenshot shows a web application window titled "Admin: [User ID]". The window has several tabs: "General", "Work Info", "Contact Info", "Regulations", "Administration", "Business roles", and "IAM roles". The "Administration" tab is selected. The main content area contains a list of administrative actions, each with a checkbox:

- Suspend the account
- Deprovision account
- Organization suspended
- Reset password**
- Initial password
- Unlock account
- Preserve Roles
- Roles History
- Groups History
- AD Groups History
- Office Phone History
- Mobile Phone History
- Active Directory location
- Active Directory location

The "Reset password" checkbox is highlighted with a red rectangular box.

Figure 19: 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 Auditor	Interact Portal	NEA 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 NEA Audit Guideline). The NEA Auditor can view audit records in the application and use messaging to a limited extent.
2	NEA FocalPoint	Interact Portal	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 Interact Portal they have access to messaging, view news feed and help files.
3	NEA Inspector	Interact Portal	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 PIC 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 REACH 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.
		Interact Portal	(3) Simple and advanced search, simple view, activity pages, Substance report, stored queries, favourites elements, News Feed and Home page customisations.
		REACH-IT	(4) 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.
8	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.
9	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.
10	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.
11	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.
12	PCN Normal	Poison Centres Notifications	Access to remote folder for poison centres notifications to download one or multiple notifications.
13	Appointed Body Interact Portal	Interact Portal	Access to the PCN database through Interact Portal for Appointed Bodies or Poison Centres.
14	MSCA POPs	Interact Portal	Access to ACT, the POPs reporting module, news feed (POPs) and help (POPs)
15	EEA/EFTA POPs	Interact Portal	Access to the POPs reporting module, news feed (POPs) and help (POPs)
16	EC POPs	Interact Portal	Access to ACT, access to all data across all MS and EEA/EFTA in the POPs in the reporting module, access to news feed (POPs) and help (POPs)
17	NEA BPR Auditor	Interact Portal	This role provides access to My Dashboard page, can read News related to BPR, access Help page and Help Files for BPR and is the only role with access to Auditing pages. Each NEA BPR Auditor has access to auditing pages related only to own Member State
18	NEA BPR Focal Point	Interact Portal	This role is about the recipient of a message from ECHA or NEA BPR Inspector of same Member State. This role provides access to My Dashboard page, News portlet (BPR Section), Messaging, Help Page and Help File for BPR.

19	NEA BPR Inspector	Interact Portal	This role provides access to My Dashboard page, News portlet (BPR Section), Data Search for Biocides, Messaging, Help page and Help Files for BPR. This role provides no access to Auditing pages.
<p>The following roles are meant only for User Administration purposes (access to the IAM portal – not to the other IT tools)</p>			
20	NEA Administrator	IAM Portal	Create/delete users, provision/deprovision business roles and request services for Enforcement users.
21	MSCA user administrator	IAM Portal	Create/delete users, provision/deprovision business roles and request services for Competent Authorities' users.
22	PCN user administrator	IAM Portal	Create/delete users, provision/deprovision business roles and request services for Appointed Bodies and Poison Centres.

In the Welcome screen (Figure 10: Welcome screen in the IAM portal), select **Access requests** from the left-hand side (Figure 20: Access Request).

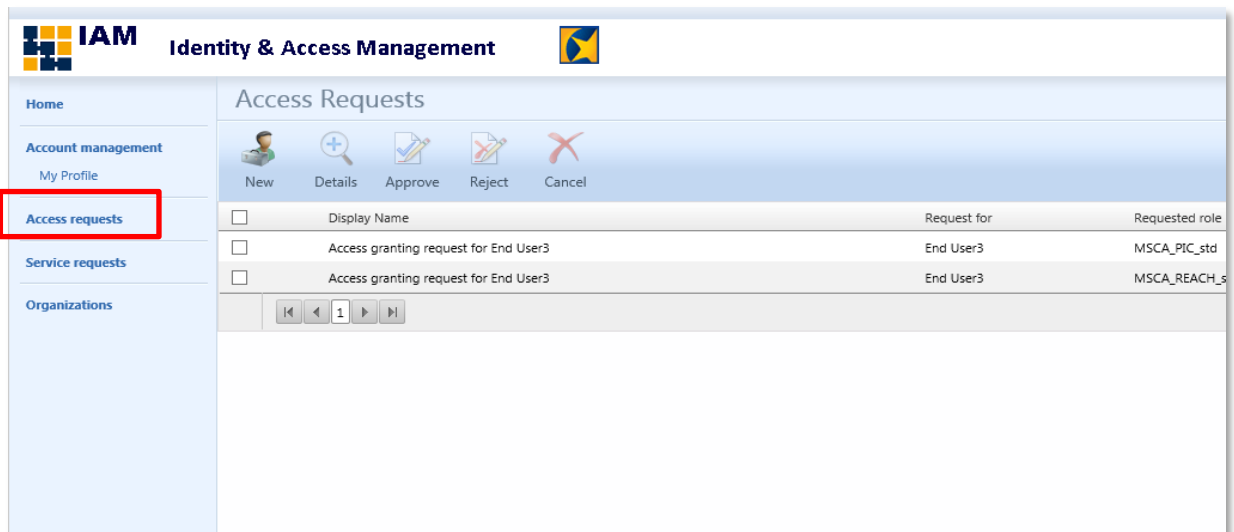


Figure 20: Access Request

Click on 'New' to create a new access request (Figure 21: New Access Request Form).

'Request type': Select either Grand a new business role or Revoke a business role. Fill

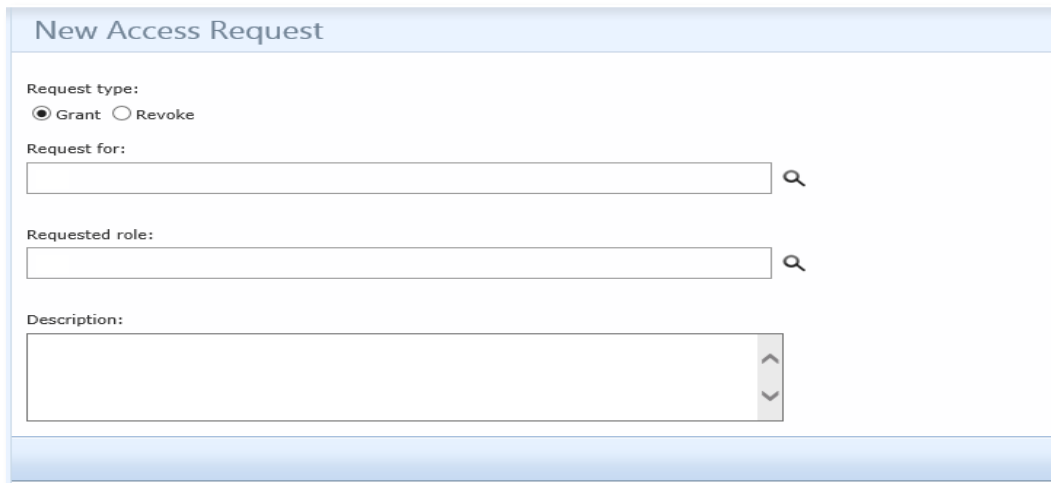
in the following fields:

'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.



The screenshot shows a web form titled "New Access Request". It contains the following elements:

- Request type:** Two radio buttons, "Grant" (which is selected) and "Revoke".
- Request for:** A text input field with a magnifying glass icon to its right.
- Requested role:** A text input field with a magnifying glass icon to its right.
- Description:** A larger text input field with a vertical scrollbar on its right side.

Figure 21: 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

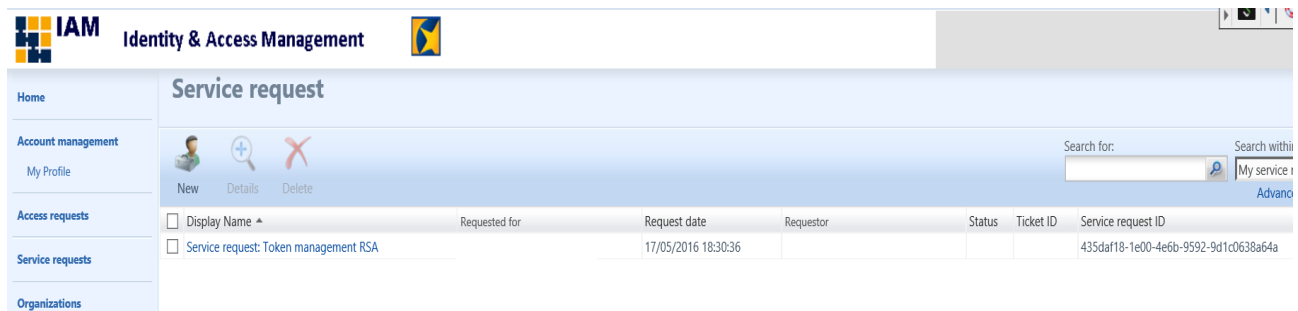
6.1 Service Request

The User Administrators can place requests for the services below:

1. RSA token management
2. Users reports in IAM

	<p>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.</p>
---	--

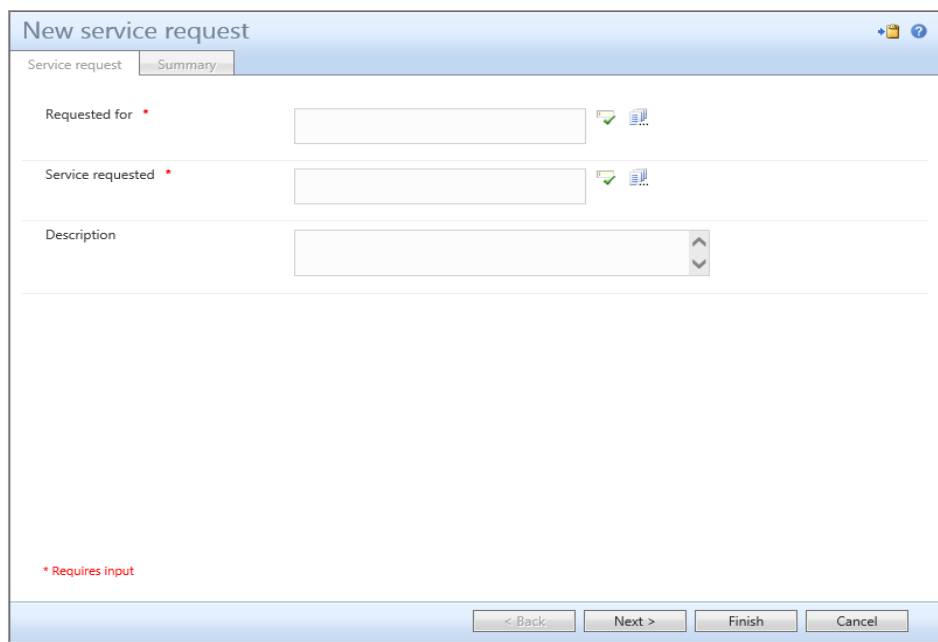
In the Welcome screen (Figure 10: Welcome screen in the IAM portal), select **Service requests** from the left-hand side (Figure 22: Service request).



Requested for	Request date	Requestor	Status	Ticket ID	Service request ID
Service request: Token management RSA	17/05/2016 18:30:36				435daf18-1e00-4e6b-9592-9d1c0638a64a

Figure 22: Service request

Click on 'New' to create a new Service request (Figure 23: New Service request).



New service request

Service request Summary

Requested for *

Service requested *

Description

* Requires Input

< Back Next > Finish Cancel

Figure 23: 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 24: Select service task).

'Description': write a small description about the request. Click on '**Save**' to finalise the process.

Select service task

Search for: Search within:

Action	Application	Category
<input type="checkbox"/> Token management	RSA	Token management

Selected Resources 1 items total Page 1 of 1

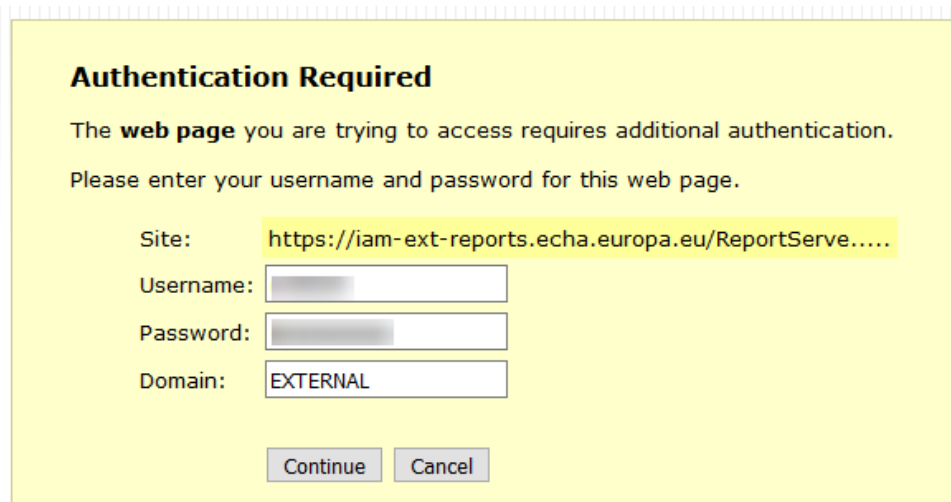
Figure 24: Select service task

7. Organization Information report

7.1 Login to the Organization Information Report

Click on 'IAM Organization Report' 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'



The screenshot shows a yellow dialog box titled "Authentication Required". The text inside reads: "The web page you are trying to access requires additional authentication. Please enter your username and password for this web page." Below this text are four input fields: "Site:" with the value "https://iam-ext-reports.echa.europa.eu/ReportServe.....", "Username:" with a blurred input field, "Password:" with a blurred input field, and "Domain:" with the value "EXTERNAL". At the bottom of the dialog are two buttons: "Continue" and "Cancel".

Figure 25: IAM Organization Report Login page

7.2 Generating a new report

After successfully logging in, please wait a couple of seconds for the report to be generated. When the report will load will be visible each regulation of the relative organization, the roles under each regulation and each user that has effective each of the roles.

Also, for each user will be noted in the column "Last account use" the last date time when the specific account accesses any ECHA tool.

Please note that by pressing the buttons (as seen in the figure 28):

- (1) you can export this report in various available formats (e.g. excel, pdf),
- (2) you can refresh the report,
- (3) you can move into the various pages of the report by using the controls.

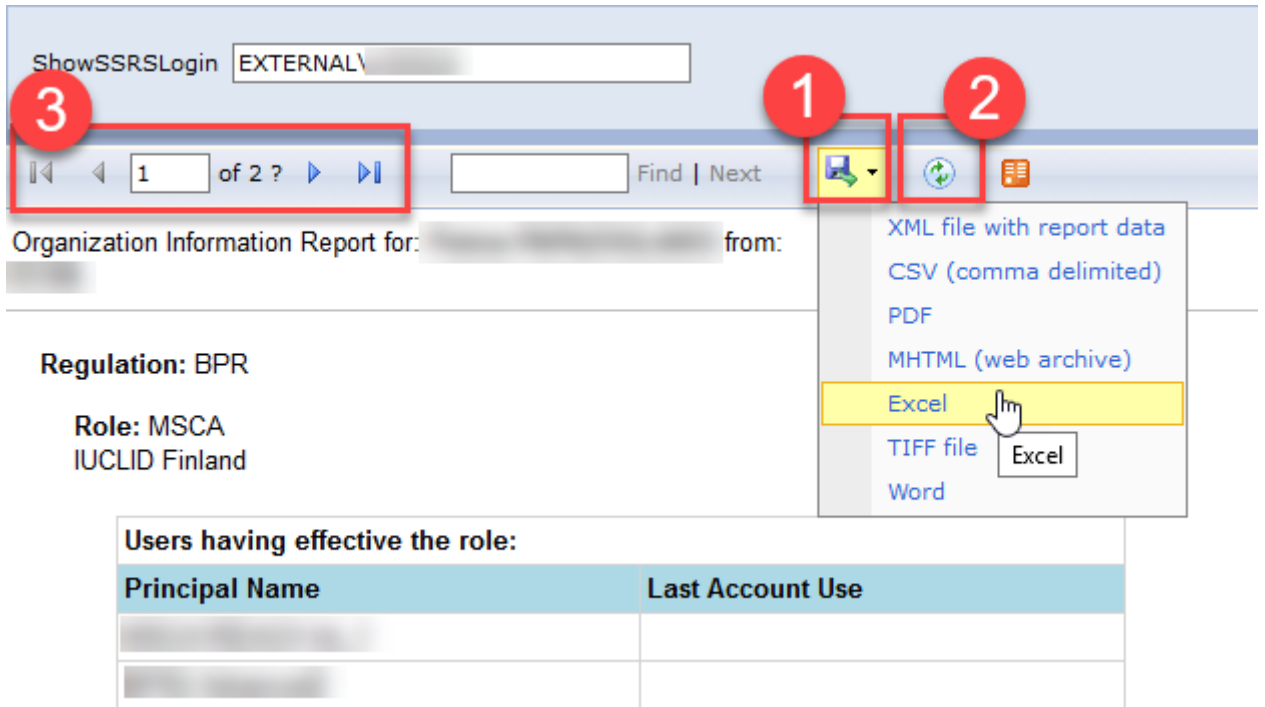



Figure 26: IAM Organization Report

8. 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/ContactFormAuthorities.aspx>

	<p>Use the option 'I can't login' to report login problems</p> <p>Use the I need support with to ask questions e.g. regarding the portal.</p>
---	---

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 minutes

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 privileges)
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 regard 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
TELAKKAKATU 6-8, P.O. BOX 400,
FI-00150 HELSINKI, FINLAND
ECHA.EUROPA.EU