

Managing access to IMI

1. WHO CAN MANAGE ACCESS TO IMI?	2
2. AUTHORITY REGISTRATION	2
2.1. REGISTERING AN AUTHORITY IN IMI	2
2.1.1. REGISTERING AUTHORITY DETAILS & THE FIRST USER	3
2.1.2. GRANTING ACCESS TO THE APPROPRIATE MODULE(S)	3
2.2. INVITING AUTHORITIES TO SELF-REGISTER	3
3. MANAGING AUTHORITIES & USERS	4
3.1. MANAGING AUTHORITIES	4
3.1.1. UPDATING BASIC DATA ON AUTHORITIES	4
3.1.2. UPDATING MODULE CLASSIFICATIONS, SETTINGS & LINKED COORDINATORS	4
3.1.3. ADDING & REMOVING ACCESS MANAGERS (MANAGEMENT INFORMATION TAB)	5
3.1.4. GRANTING & SUSPENDING ACCESS TO MODULES	5
3.2. MANAGING USERS	5
3.2.1. PASSWORD EXPIRY	6
4. GRANTING ACCESS TO A NEWLY INTRODUCED MODULE	6
5. REMOVING AN AUTHORITY FROM IMI	6



1. WHO CAN MANAGE ACCESS TO IMI?

National IMI Coordinators (known as **NIMICs**) are responsible for ensuring that the relevant authorities are registered in IMI and that they can access the modules corresponding to their areas of competence. NIMICs may delegate this responsibility – partially or wholly - to other registered authorities.

In IMI, **authorities that manage access to the system** are called **Access Managers**. As well as registering new authorities and users, and granting access to specific modules, access managers ensure that data about authorities are kept up-to-date.


Many authorities responsible for managing access are also responsible for exchanging information and/or coordinating information exchanges in IMI.

The rights assigned to users within an authority depend on their individual responsibilities. To register and manage other authorities, **a user in an Access Manager must have Administrator rights**.

2. AUTHORITY REGISTRATION

Access Managers are responsible for registering competent authorities that need to use IMI. As a user within an Access Manager with Administrator rights, you can either:

- register the authority in IMI **yourself**, or
- you can invite the authority to **self-register**.

 An authority should be **registered in IMI once only**. Before you register an authority, check if it's already registered. If it is, all you may need to do is:

- grant it access to an additional module (see section 2.1.2)
- register additional users
- and/or change the assigned roles of existing users (see sections 3.2).

If an authority is **not** yet registered, **either** register it yourself **or** send an invitation to self-register.

2.1. REGISTERING AN AUTHORITY IN IMI

As an **Access Manager** you can register a new authority using the 'Administration' menu option. There are 2 steps:


1. Enter the details of the authority and the first user
2. Grant the authority access to the appropriate modules.

2.1.1. REGISTERING AUTHORITY DETAILS & THE FIRST USER

Enter the following data:

- the authority's official name and an informal title (to make the areas for which it is responsible clear to its counterparts)
- the authority's contact details (e.g. phone number, address and website)
- the name and contact details of the first user to be registered for the authority.

Select appropriate entries from classification lists to inform counterparts about the authority's domain of responsibility.

 The first user automatically receives a temporary password by e-mail. **It is your task to tell the user his or her username.** For security reasons, you must **NOT** use e-mail for this purpose.

First users are granted Administrator rights, enabling them to:

- update the authority's details in IMI
- register, update and remove users
- reset passwords.

For further information, see the guidelines for Administrators - [Managing my authority and users](#).

You have now registered the authority and its first user in IMI. The next task is to grant access to the relevant IMI module(s).

2.1.2. GRANTING ACCESS TO THE APPROPRIATE MODULE(S)

Select the 'Modules' tab and grant access to the appropriate module(s). Depending on the module you select, you may have to:

- specify whether the authority will play a coordinating role or simply act as an authority
- select from module-specific classification lists
- specify settings for approval, the right to refuse and allocation (for information requests only)
- select a linked coordinator (only if the authority is **not** assigned a coordinating role for the module).

The user you have already registered automatically has all user rights for the module(s) selected.

2.2. INVITING AUTHORITIES TO SELF-REGISTER

Inviting authorities to self-register can cut your workload while maintaining your overall control of the registration process. An authority can only self-register on receipt of an invitation from an Access Manager.

There are **4 steps** in this process:

1. As an Access Manager, you create and submit the invitation to register. Select the menu option 'Administration' → 'Invitations to register'.
2. The competent authority receives the invitation and records its data in the system.
3. As an Access Manager, you will be automatically notified by e-mail each time an authority registers. You must validate the data entered by the authority. Select the menu option 'My tasks' → 'Pending validations' to view the registration.
4. Select the 'Modules' tab to grant the authority access to the relevant IMI modules.

1. Invite authority to register → 2. Authority registers itself → 3. Validate registration → 4. Grant access to modules

3. MANAGING AUTHORITIES & USERS

When you register an authority in IMI you automatically become its Access Manager and appear on its 'Management Information' tab. **You can update its data and users** using the 'Administration' → 'Managed Authorities' menu option. The authority search criteria available under this option returns only authorities for which you are an Access Manager. You can also use this menu option to manage other authorities and users in your country - select 'No' in response to the search criterion 'My authorities only'.

3.1. MANAGING AUTHORITIES

3.1.1. UPDATING BASIC DATA ON AUTHORITIES

Data on authorities must be kept up to date in IMI so that other authorities can easily identify their counterparts. To update an authority's basic data:

1. Identify the authority using the 'Managed authorities' menu option.
2. Open the authority's details.
3. The '**Authority**' tab provides the '**Edit authority**' button. This also allows you to edit certain data on the 'Classification', 'Modules' and 'Management information' tabs.

3.1.2. UPDATING MODULE CLASSIFICATIONS, SETTINGS & LINKED COORDINATORS

To modify information relating to a module:

1. Select '**Edit authority**' on the '**Authority**' tab.
2. Go to the '**Modules**' tab.
3. Select the module.
4. Modify the classification, settings and/or linked coordinators.

3.1.3. ADDING & REMOVING ACCESS MANAGERS (MANAGEMENT INFORMATION TAB)

The 'Management information' tab displays the following information about an authority in IMI:

- its status (active or suspended)
- its Access Managers
- a history of updates
- a list of the authority's users with Administrator rights.

Again, the **'Edit authority' button on the 'Authority' tab** enables you to add your authority as an Access Manager. This makes it easier for you to manage the authority, as it will be included in the default search criteria for the 'Managed authorities' and 'Send e-mail' menu options.

3.1.4. GRANTING & SUSPENDING ACCESS TO MODULES

To grant or suspend an authority's access to a particular module:

1. Identify the authority via the 'Managed authorities' menu option.
2. Open the authority's details.
3. Select the **'Modules' tab**.

When granting access to certain modules, you must also select a linked coordinator. When you grant access to a new module, IMI automatically assigns all user roles for the module to any Administrators within the authority. You may need to **assign roles for the module to other existing users or to register new users for the module**.

To change an authority's role for a given module from 'Authority' to 'Coordinator' (or vice-versa), you must first suspend its access to the module.

3.2. MANAGING USERS


As well as maintaining data about authorities, you can also manage their users. You may:

- register new users
- change the usernames assigned automatically (once the registration is completed)
- change user rights (assigning and removing roles for different modules)
- reset passwords
- remove users.

To manage users:

1. Find the relevant authority using the 'Administration' → 'Managed authorities' menu option.
2. Open the authority's details.

3. Select the **'Users' tab**.
4. A list of registered users appears. You can now edit their details or reset passwords¹.

 When you register a new user, he or she automatically receives a temporary password by e-mail. **It is your task to tell the user his or her username.** For security reasons, you must **NOT** use e-mail for this purpose.

3.2.1. PASSWORD EXPIRY


Passwords should be changed every 6 months. Users will receive a reminder by email.²

As an Access Manager you can see:

- whether a user has logged in at least once (status: **active**)
- has never logged in (status: **new**)
- whether the user has a temporary, valid, blocked or expired password.

4. GRANTING ACCESS TO A NEWLY INTRODUCED MODULE

When a **new module is added to IMI**, it may be your duty to identify the authorities that will need to use it. Alternatively, someone else may be responsible for identifying the relevant authorities, while it remains your task to grant them access in IMI.

 Once these authorities are **identified, check whether they are already registered in IMI**. If an authority is already registered for an existing module, simply add access to the new module under the 'Modules' tab (see section 3.1.4). If an authority is **not** yet registered in IMI, either register it yourself or send it an invitation to self-register (see section 2.1).

5. REMOVING AN AUTHORITY FROM IMI

To remove an authority:

1. **Suspend its access to all modules.**

You can suspend access to modules, one by one, on the **'Modules' tab**. When you suspend access to a given module the authority will be able to complete any on-going exchanges in

¹ When you reset a password, the system emails the user a temporary password.

² Passwords must comply with the following rules:

- The last 5 passwords cannot be used
- A password must have at least 8 characters
- It must contain at least: 1 uppercase character, 1 lowercase character, 1 numerical digit.

that module but will not be able to initiate or receive new exchanges. You can at anytime re-grant the authority access to the suspended module.

2. **Deactivate the authority** on the '**Authority**' tab. This means it cannot receive any new requests or notifications from other authorities, and will not be retrieved by the general 'Authorities' → 'Search' menu option.
3. Unless you 'reactivate' the authority, it will be **deleted** from IMI **6 months after deactivation**.

1. Suspend access to all modules → 2. Deactivate authority → 3. Authority automatically deleted

If you need to **reactivate** the authority **before it is deleted**, use the 'Authority' tab. Then reinstate its access to the appropriate modules to enable it to share information.